DHBW
Duale Hochschule
Baden-Württemberg
Stuttgart

KOS.content

01 | 2014

Ergebnisse der Untersuchungen des
Kompetenzzentrum Open Source der DHBW-Stuttgart

Frühjahr 2014
band.1

Editorial

Lieber Leser,

vor Ihnen liegt der erste Ergebnisband mit studentischen Ausarbeitungen, die im Rahmen des Forschungsprojekt KOS entstanden sind. KOS steht für Kompetenzzentrum Open Source und bezeichnet ein kooperatives Forschungsprojekt im Studiengang Wirtschaftsinformatik der DHBW Stuttgart, das in Zusammenarbeit mit den dualen Partnern Allianz Deutschland, HALLESCHE Krankenversicherung und Deutsche Rentenversicherung Baden-Württemberg den Einsatz von Open Source Software/Techniken zur Optimierung von Geschäftsprozessen in Versicherungsunternehmen untersucht.

Die Ursprünge des Forschungsprojekts KOS gehen auf das Jahr 2009 zurück, in dem die Duale Hochschule Baden-Württemberg (DHBW) nicht nur den Hochschulstatus erhielt, sondern damit verbunden auch einen Forschungsauftrag. Im Studiengang Wirtschaftsinformatik startete man damals zwar sofort mit den ersten Überlegungen zu möglichen Formen der kooperativen Forschung, es dauerte dann aber doch noch zwei Jahre, bis man sich mit drei dualen Partnern einig darüber war, wie eine Zusammenarbeit auf Forschungsebene aussehen könnte.

Die zwei Vorbereitungsjahre haben dem Projekt gut getan. Denn innerhalb kürzester Zeit entwickelte sich im Projekt KOS eine Form der lehreintegrierten kooperativen Forschung wie es sich alle Beteiligten idealerweise vorgestellt hatten:

Die dualen Partner liefern aus deren betrieblichen Abläufen heraus die zu untersuchenden Fragestellungen, wobei es oft um einen Vergleich des Einsatzes kommerzieller Software mit dem Einsatz von Open-Source-Produkten geht. Die jeweiligen Fragestellungen werden dann in Seminaren an der DHBW von studentischen Arbeitsgruppen analysiert, wobei nicht nur die Dozenten, sondern auch Fachexperten der dualen Partner die Studierenden wissenschaftlich leiten.

Am Ende eines jeden Seminars präsentieren die Studierenden die Untersuchungsergebnisse vor den Vertretern der beteiligten Unternehmen. Meist geht dabei um generische Lösungskonzepte, die von den beteiligten dualen Partnern in konkrete Lösungen für das eigene Unternehmen umgesetzt werden können. Diese Abschlusspräsentationen sind nicht nur für die Unternehmen, sondern auch für die Studierenden etwas Besonderes, da sie ihre Seminarergebnisse vor einem recht großen fachkundigem Publikum „verkaufen" müssen.

Ein halbes Jahr nach den Ergebnispräsentationen werden die studentischen Ausarbeitungen schließlich in Form eines Sammelbandes veröffentlicht. Das vorliegende Dokument ist der erste Band in dieser Reihe und fasst die Ergebnisse aus dem Seminar im Wintersemester 2013/2014 zusammen. Weitere Bände werden semesterweise folgen, nicht zuletzt deshalb, weil die dualen Partner im Dezember 2013 das zweijährige Projekt KOS um zwei weitere Jahre verlängert haben.

Wir wünschen allen Lesern eine spannende Lektüre und hoffen, dass der vorliegende Sammelband viele interessante Erkenntnisse aus dem Open-Source-Bereich für Sie bereithält.

Prof. Dr. Niko Preiß _ Wissenschaftlicher Leiter
Dipl.-Inform. Michael Hitz _ Projektleiter
Prof. Dr. Thomas Kessel _ Wissenschaftlicher Leiter

INHALT BAND.1

Das Kompetenzzentrum Open Source (KOS)

Ziel des Projektes

Das Projekt Kompetenzzentrum Open Source der DHBW Stuttgart wurde mit der Zielsetzung ins Leben gerufen, die Einsatzfelder für Open Source Software in Unternehmen zu identifizieren und durch den Einsatz quelloffener Produkte und deren kostengünstigen Einsatzmöglichkeiten Optimierungen in ausgewählten Geschäftsbereichen zu erzielen.

Dies bedeutet konkret, dass z.B. Open Source Software evaluiert wird, um Lizenzkosten zu reduzieren, bewertet wird, ob sie diverse Qualitätskriterien erfüllt und erfolgreich(er) und effizient(er) in Unternehmen genutzt werden kann. Das Ziel des Projektes ist es hierbei, allgemeingültige Lösungskonzepte für Problemstellungen zu erarbeiten, welche von den am Projekt beteiligten Unternehmen zu firmenspezifischen Lösungen weiterentwickelt werden können. Die beteiligten Unternehmen partizipieren so an den Ergebnissen des Projekts.

Zusammenarbeit mit den Dualen Partnern

Die Zusammenarbeit mit den Dualen Partnern gestaltet sich entlang deren Anforderungen und Bedürfnissen. Sie sind die Themengeber für betriebliche Fragestellungen, die im Rahmen des Projekts untersucht werden. Die DHBW steuert die wissenschaftliche, didaktische und methodische Expertise und Forschungskompetenz bei und untersucht die identifizierten Themenfelder.

Im Rahmen des Projektes steuert die DHBW Stuttgart die wissenschaftliche Expertise und Forschungskompetenz bei zur Bearbeitung der betrieblichen Fragestellungen der Dualen Partner. Es entstehen generische Lösungen, welche von den Partnern an Ihre Situation angepasst werden kann.
Im Rahmen der Arbeit entstehen (generische) Lösungen, an denen die Partner teilhaben können indem sie diese auf ihre spezifische Unternehmenssituation anpassen. Zudem fließen die Ergebnisse in die Arbeit der DHBW ein, sodass hier dem Anspruch an eine hohe Anwendungs- und Transferorientierung ganz im Sinne einer kooperativen Forschung Rechnung getragen wird.

An den Ergebnissen des Projekts partizipieren die Dualen Partner Allianz Deutschland AG, die Deutsche Rentenversicherung Baden-Württemberg und die HALLESCHE Krankenversicherung a.G.

DHBW
Duale Hochschule
Baden-Württemberg
Stuttgart

Automatisierung von Geschäftsprozessen mithilfe von Workflow-Management-Systemen

Modellierung eines praxisnahen Beispiels mit dem Tool camunda

Schriftliche Ausarbeitung
im Rahmen der Lehrveranstaltung „Integrationsseminar“

am 31.01.2014

Fakultät Wirtschaft
Studiengang Wirtschaftsinformatik
WWI2011V

Inhaltsverzeichnis

Abkürzungsverzeichnis

API:	Application-Programming-Interface
BPEL	Web Service Business Process Execution Language
BPMN	Business Process Model and Notation
DN:	Distinguished Name
HTML:	Hypertext Markup Language
LDAP:	Lightweight Directory Access Protocol
REST:	Representational State Transfer
SSL:	Secure Sockets Layer
URI:	Unique Resource Identifier
URL:	Uniform Resource Locator
VBA:	Visual Basic Application
WfMC	Workflow Management Coalition
XML:	Extensible Markup Language

Abbildungsverzeichnis

Tabellenverzeichnis

1 Optimierte Ablaufsteuerung durch Workflow-Management

In der betrieblichen Praxis werden stark administrative Aufgaben häufig manuell ausgeführt. Besonders das Verwalten, Bearbeiten und Versenden von Informationen ist ein iterativer, stark strukturierter Prozess, welcher mithilfe von Workflow-Management automatisiert werden kann.

1.1 Motivation

In Unternehmen aller Branchen werden Verwaltungsprozesse durchlaufen. Die Koordination und Kontrolle der einzelnen Aufgaben dieser Prozesse, sowie die Steuerung und Einhaltung des Ablaufes werden oft immer noch von Mitarbeitern manuell durchgeführt. Werden bei der Realisierung dieser Aufgaben Tools verwendet, die lediglich das Speichern und Dokumentieren der Informationen unterstützen, übernimmt der Mitarbeiter weiterhin einen Großteil der Ablaufsteuerung. Nutzt man die Eigenschaft, dass Verwaltungsprozesse überwiegend strukturiert und iterativ stattfinden, können Workflow-Management-Systeme diese Aufgaben der Mitarbeiter automatisieren. Dabei können zusätzlich erweiterte Funktionen, wie die Datenaufbereitung zur Laufzeit, genutzt werden.
Dieser Wunsch nach einer Entlastung der Mitarbeiter bei der Erfüllung administrativer Aufgaben ist der Anlass, weshalb sich die vorliegende Arbeit im Rahmen der KOS-Projekte mit der Automatisierung von Verwaltungsprozessen beschäftigt.

1.2 Zielsetzung

Die Zielgruppe dieser Arbeit sind Unternehmen, die einen oder mehrere ihrer Verwaltungsprozesse automatisieren möchten. Besonders vor der Einführung von Workflow-Management-Systemen ist es wichtig, sich mit den Grundlagen des Workflow-Managements und der Funktionsweise einer Workflow-Engine zu beschäftigen.
Diesem Gedanken folgend gliedert sich die vorliegende Arbeit in die Einführung in das Workflow-Management, die Auswahl und Installation eines geeigneten Tools zur Umsetzung und in die Einführung in die Arbeit mit diesem. Aufbauend auf diesen Kenntnissen wird anhand eines Beispielprozesses gezeigt, wie sich grundlegende Konzepte mit dem Tool modellieren lassen. Der schrittweise Aufbau ermöglicht dem Leser zu erlernen, wie sich Lösungen für praktische Anforderungen umsetzen lassen. Die Komplexität der Ansätze wird dabei kapitelweise gesteigert. Anschließend zeigen weiterführende Konzepte, wie individuelle oder branchenspezifische Problemstellungen durch Anbinden eigenständig implementierter Funktionalitäten gelöst werden können. Die Dokumentation betrachtet zusätzlich, wie ein unternehmensspezifisches Frontend an die Workflow-Engine angebunden werden kann.

Die vorliegende Arbeit ist als Leitfaden für den Einsatz von Workflow-Management-Systemen gedacht. Die theoretischen Grundlagen und die Installationshilfe des Tools camunda geben auch Neulingen auf den Gebiet Workflow-Management die Möglichkeit, Prozesse zu automatisieren.

Ziel dieser Arbeit ist somit praxisnah darzulegen, wie die Modellierung, Ausführung und das Monitoring von Prozessen mithilfe von Workflow-Management-Systemen optimiert werden können.

2 Modellieren von Workflows durch Workflow-Management

Das Kapitel 2 beschäftigt sich anfangs mit den notwendigen Grundlagen zu Workflow-Management. Anschließend werden die Workflowmodellierungssprachen BPEL und BPMN vorgestellt.

2.1 Grundlagen des Workflow-Managements

Bevor die konkrete Modellierung eines Prozesses möglich ist, ist es notwendig, das Vorgehen des Workflow-Managements zu verstehen. Im Folgenden werden nicht nur die Definition und die Ziele des Workflow-Managements, sondern auch der Einsatz von Workflow-Management-Systemen und deren Aufbau erläutert. Die darauffolgende Abgrenzung und Unterteilung von Workflows zeigt die Verbesserungspotenziale, bei denen der Einsatz von Workflow-Management sinnvoll ist.

2.1.1 Eingrenzung und Definition

Rasante Veränderungen und ständig steigende Anforderungen sind Gründe, weshalb Unternehmen ihre Stellung gegenüber anderen Wettbewerbern auf dem Markt ständig überprüfen müssen. Denn Wettbewerbsvorteile können nur dann erzielt werden, wenn Unternehmen frühzeitig auf Änderungen reagieren können. Zur Erreichung einer solch hohen Flexibilität und kurzen Reaktionszeiten ist der Einsatz von Prozess-Management in der Unternehmensgestaltung unausweichlich geworden.
„Prozess-Management ist ein zentraler Bestandteil eines integrierten Konzeptes für das Geschäftsprozess- und Workflow-Management. Es dient dem Abgleich mit der Unternehmensstrategie, der organisatorischen Gestaltung von Prozessen, sowie deren technischer Umsetzung mit geeigneten Kommunikations- und Informationssystemen.“[1] Die **Entwicklung der Unternehmensstrategie** findet auf der strategischen Ebene des Unternehmens statt. Sie umfasst die Betrachtung aller Geschäftsfelder des Unternehmens und leistet so einen Beitrag zum Unternehmenserfolg.[2] Auf der darunterliegenden, fachlich-konzeptionellen Ebene findet die Ableitung der Strategie auf die einzelnen Geschäftsprozesse statt, deren Koordination durch das **Geschäftsprozess-Management** gewährleistet wird. Auf der untersten Ebene, der operativen Ebene, stellt das **Workflow-Management** die Durchführung und Anbindung an Anwendungs- und Informationssysteme sicher. Die folgende Abbildung 1 verdeutlicht den eben beschriebenen Zusammenhang.

[1] Gadatsch, A. (2010), S. 1
[2] Vgl. Österle, H.(1995), S.130

Strategieentwicklung — strategische Ebene

Geschäftsprozess-Management — fachlich-konzeptionelle Ebene

Workflow-Management — operative Ebene

Abb. 1: Einordnung Workflow-Management im Unternehmen[3]

Der Fokus der vorliegenden Seminararbeit liegt auf dem Workflow-Management. Um dem Leser eine genauere Definition zu ermöglichen, sollen anhand der Abbildung 2 die Aufgaben und Ziele von Geschäftsprozess- und Workflow-Management abgegrenzt werden.

	Geschäftsprozess-Management	Workflow-Management
Ziel	Inhaltliche Gestaltung der Arbeitsabläufe zur Umsetzung der strategischen Unternehmensziele	Unterstützung der operativen Ausführung von Prozessen durch Umsetzung der Geschäftsprozessziele
Ebene	Konzeptionell-fachlich	Operativ
Aufgabenschwerpunkt	Neugestaltung und Optimierung der Geschäftsprozesse zur Erreichung der Geschäftsstrategieziele	Voll- oder teilautomatisierte Umsetzung der Geschäftsprozesse im Rahmen der Ziele der Geschäftsstrategie

Abb. 2: Abgrenzung Geschäftsprozess- und Workflow-Management[4]

Ziel im Geschäftsprozess-Management ist es, die Gestaltung der Arbeitsabläufe innerhalb des Unternehmens so zu gestalten, dass deren Umsetzung die Unternehmensstrategie verfolgt. Zudem können eine systematische Steigerung der Prozessleistung, sowie eine Reduktion des Koordinationsaufwands und der Anzahl der Schnittstellen erzielt werden.[5] Das Ergebnis von Geschäftsprozess-Management sind somit neugestaltete und optimierte Geschäftsprozesse, die sich durch geringere Kosten, höhere Geschwindigkeit und verbesserte Flexibilität auszeichnen.[6] Die Prozesse haben den erforderlichen Detaillierungsgrad erreicht, wenn die einzelnen Aktivitäten soweit untergliedert sind, dass sie einem bestimmten Mitar-

[3] Mit Änderungen entnommen aus: Gadatsch, A. (2010), S. 2
[4] Mit Änderungen entnommen aus: Gadatsch, A. (2001), S. 41
[5] Vgl. Schmelzer, H. J./Sesselmann, W. (2003), S. 68 f.
[6] Vgl. Hammer, M.(2010), S. 7

beiter zugeordnet werden können, sodass kein weiterer Wechsel des Bearbeiters mehr erforderlich ist.[7]

Auf der operativen Ebene können nun die Prozesse mit Hilfe von Workflow-Management so beschrieben werden, dass die ausführenden Mitarbeiter eine konkrete Arbeitsanweisung erhalten bzw. die Vorgabe für computergestützte Arbeiten als strukturierter, ausführbarer Ablauf für ein Anwendungssystem vorliegt. Auf Workflow-Ebene wird somit auch die Konkretisierung hinsichtlich personeller und technischer Ressourcen vorgenommen.[8]

Zusammenfassend richtet sich das Geschäftsprozess-Management somit nach der Geschäftsstrategie; das Workflow-Management unterstützt die auf der fachlich-konzeptionellen Ebene festgelegten Geschäftsprozessziele.

2.1.2 Phasen und Ziele

Ausgehend von der Abgrenzung aus Kapitel 2.1.1 wird in diesem Kapitel die genaue Definition des Begriffs Workflow-Management eingeführt. Das Workflow-Management umfasst auf der operativen Ebene die Phasen der Modellierung, der Ausführung und des Monitorings:

Abb. 3: Phasen des Workflow-Managements

Bei der Modellierung eines Workflows wird der auf fachlich-konzeptioneller Ebene erstellte Geschäftsprozess in eine detaillierte Spezifikation auf technischer Ebene überführt.[9] Die anschließende Phase der Workflow-Ausführung beinhaltet die Erzeugung und den Durchlauf von Prozessinstanzen entlang des strukturierten und definierten Ablaufs. Das Monitoring dient der laufenden Überwachung und Auskunftsfähigkeit über die durchlaufenen Prozesse. Durch den Vergleich der aus dem Monitoring entnommenen Werte und der geplanten Werte ist eine zeitnahe Korrektur des Ablaufs möglich.

Mit dem Durchlaufen dieser drei Phasen des Workflow-Managements, verfolgen Unternehmen verschiedene **Ziele**:[10]

- **Unterstützung**: Unternehmen erwarten Unterstützung bei der konkreten, technischen Umsetzung eines Prozesses.
- **Prozesstransparenz**: Mithilfe von Workflow-Management können Informationen über geplante und aktuell ausgeführte Prozesse in Echtzeit abgerufen und aufbereitet

[7] Vgl. Füermann, T./Dammasch, C.(2008), S. 9
[8] Vgl. Gadatsch, A.(2001), S. 35
[9] Vgl. Müller, J.(2011), S. 9
[10] Vgl. Gadatsch, A.(2001), S. 38 ff.

werden. Zusätzlich ist eine verbesserte Auskunftsmöglichkeit über beispielsweise den Status oder den aktuellen Bearbeiter möglich. Auch für zukünftige Prozesse können die Aufzeichnung von Unterbrechungen und Überschreitungen von Grenzwerten einen Teil zur Verbesserung beitragen.

- **Durchlaufzeiten**: Durch eine optimierte Ablaufsteuerung können die Durchlaufzeiten minimiert werden. Dabei spielen vor allem die Zuordnung der Bearbeiter und der automatisierte Aufruf eines Programms eine Rolle.
- **Organisatorische Änderungen**: Die Geschäftsprozesse von Unternehmen ändern sich ständig. Eine permanente Anpassung der Arbeitsabläufe auf operativer Ebene soll durch Workflow-Management weiterhin ohne zu großen Aufwand möglich sein.
- **Automatisierung**: Das informationstechnische Ziel ist teil- bzw. vollautomatisierte Unterstützung der Durchführung von Arbeitsabläufen. Workflow-Management ermöglicht nicht nur die Automatisierung eines Teilprozesses, sondern unterstützt die zusammenhängenden Teilprozesse eines Gesamtprozesses. Somit ist es beispielsweise für einen Bearbeiter nicht mehr nötig, Vor- und Nachgänger der auszuführenden Aktivität zu kennen, weil auch der Ablauf technisch vorgegeben ist.

Diese Ziele können durch den Einsatz von Workflow-Management-Systemen erreicht werden.

2.1.3 Workflow-Management-Systeme

„Workflow-Management-Systeme sind Softwaresysteme, deren Kernaufgabe die Unterstützung betrieblicher Prozessabläufe durch die Koordination von Aktivitäten, Anwendung, Daten und prozessbeteiligten Personen ist.“[11] Sie unterstützen also die in Abbildung 3 aufgeführten Phasen und können zusätzlich Funktionen, wie die Simulation, eine Ablaufalternative oder die Analyse von Workflows übernehmen. Mit Hilfe eines Programmes können Workflows in einem solchen System modelliert, erzeugt und zur Laufzeit verwaltet und interpretiert werden. Das Workflow-Management-System muss eine hohe Interaktionsfähigkeit aufweisen, damit über den gesamten Prozess die Möglichkeit besteht, über eine Benutzeroberfläche mit dem Anwender zu kommunizieren. Eine weitere Aufgabe ist die Koordination des Einsatzes von Mitarbeitern und Anwendungssystemen.
Für bessere Vergleichsmöglichkeiten und Wiederverwendbarkeit ist es sinnvoll, die Standardisierungen im Bereich von Workflow-Management-Systemen zu berücksichtigen. Kapitel 2.1.4 erläutert deshalb das Workflow-Referenzmodell.

[11] Mühlen, M. zur/Hansmann, H.(2008), S. 373

2.1.4 Workflow-Referenzmodell

Seit ihrer Gründung im Jahr 1993 befasst sich die Workflow-Management Coalition (WfMC), ein Zusammenschluss aus Anwendern, Entwicklern, Analysten, sowie Forschungsgruppen, mit Geschäftsprozess- und Workflow-Management.[12] Sie hat ein Referenzmodell zur Beschreibung der Schnittstellen in einem Workflow-Management-System eingeführt. Das Ziel dieses Standards ist die Verbindungsfähigkeit und Interoperabilität zwischen den Workflows verschiedener Anbieter.[13] Manuell ausgeführte Aktivitäten werden nicht von allen Workflow-Management-Systemen gesteuert bzw. kontrolliert; dies beschränkt sich auf alle automatisiert ablaufenden Aktivitäten. Das Workflow-Referenzmodell, welches in der Abbildung 4 dargestellt ist, enthält fünf Schnittstellen (Interfaces). Das zentrale Element ist der Workflow-Ausführungsservice (Workflow Enactment Service), der aus einer oder mehreren Workflow-Engines besteht. „Eine **Workflow-Engine** ist eine Softwarekomponente, die eine Laufzeitunterstützung für die Ausführung von Workflows zur Verfügung stellt. Sie generiert aus den Prozessdefinitionen Instanzen und arbeitet die[se] unter Einbeziehung von […] Werkzeugen ab."[14] Über Programmierschnittstellen (Workflow Application Programming Interface (API) and Interchange formats), die dem einheitlichen Funktionsaufruf zwischen Systemkomponenten und der Anpassung des Formats dienen, und weitere Schnittstellen interagiert der Ausführungsservice mit fünf weiteren Komponenten.[15]

[12] Vgl. WfMC (o.J.)
[13] Vgl. Gierhake, O.(2000), S. 64
[14] Gadatsch, A.(2010), S. 257
[15] Vgl. Gadatsch, A.(2001), S. 48

Abb. 4: Referenzmodell der WfMC[16]

Die einzelnen Interfaces aus der obigen Abbildung 4 sollen in der folgenden Aufzählung erläutert werden:[17]

- **Interface 1**: Da eine hohe Anzahl verschiedener Werkzeuge und Modellierungstools zur Prozessbeschreibung vorhanden ist, empfiehlt die WfMC hier eine standardisierte Schnittstelle zu den operativen Workflow-Engines. Über ein Metamodell zur Beschreibung der Prozesse soll die Anbindung der Tools ermöglicht werden. Zum Beispiel definiert das Interface 1 die konkreten Bedingungen und Voraussetzungen für den Start, das Ende und die Funktionen eines Workflows.
- **Interface 2**: Das Interface 2 stellt den einheitlichen Austausch zwischen Anwender und dem Ausführungsservice sicher. Dieser Austausch entspricht der Abwicklung gewisser Notifikationsdienste (Workflow Client Applications). In der Praxis bedeutet dies, dass die Workflow-Engine den einzelnen Bearbeitern die jeweilige Instanz zuteilt und nach der Bearbeitung weiterleitet. Die Engine hat Zugriff auf alle Clients, die diesen Standard unterstützen, und kann somit die Ablaufsteuerung übernehmen.
- **Interface 3**: Der Umsetzungsdienst (Workflow Enactment Service) ermittelt zur Laufzeit benötigte Applikationen und Programme und stellt diese in Form von Workflow-

[16] Mit Änderungen entnommen aus: Gierhake, O.(2000), S. 65
[17] Vgl. Gadatsch, A.(2001), S. 48

Engines dem Endbearbeiter über das Interface 3 zur Verfügung. So werden voll- oder teilautomatisierte Workflows, wie beispielsweise Hostanwendungen, unterstützt.

- **Interface 4**: Das Interface 4 standardisiert die Interoperabilität, also die Fähigkeit zur Zusammenarbeit zwischen einer Engine mit weiteren Engines. Ziel ist es, durch dieses Interface auch einen unternehmensübergreifenden Austausch von Workflow-Instanzen unterschiedlicher Hersteller zu ermöglichen.
- **Interface 5**: Über die Steuerungsanwendung (Administration & Monitoring Tools) wird das Überwachen (Monitoring) und Analysieren der operativen Workflow-Instanzen und das Bearbeiten von prozessübergreifenden Verwaltungsfunktionen möglich.[18] Die Verwaltung von Benutzern und deren Rechten, die auch zu diesen Funktionen zählt, wird im weiteren Verlauf der Arbeit erläutert und anhand von Beispielen erklärt.

Durch den Einsatz des Referenzmodells der WfMC können Unternehmen die genannten Vorteile nutzen. Gerade bei der Einführung neuer Prozesse können die Standards ohne größeren Aufwand in die Modellierung der Workflows einfließen.

2.1.5 Workflow

Im den vorhergehenden Kapiteln ist bereits häufig der Begriff „Workflow" verwendet worden. Eine genaue Begriffsklärung und Unterscheidung des Workflows anhand von Kriterien soll im Folgenden vorgenommen werden.

Die WfMC definiert den **Workflow** als eine vollständige oder partielle Automatisierung eines Geschäftsprozesses, in der Dokumente, Informationen oder Aufgaben von einem Beteiligten zu einem anderen zur Realisierung übergeben werden, wobei eine Reihe von prozeduralen Regeln beachtet werden muss.[19]

Ein Workflow ist also ein inhaltlich abgeschlossener, ganz oder teilweise automatisiert ablaufender Prozess. Er enthält alle technischen, fachlichen und zeitlichen Informationen, die für die automatische Ablaufsteuerung des Prozesses auf der operativen Ebene notwendig sind. Die einzelnen anzustoßenden Aufgaben innerhalb des Prozesses, auch Tasks genannt, werden entweder manuell, durch einen Mitarbeiter, oder automatisiert, durch ein Programm, bearbeitet.[20]

Anhand der Kriterien Strukturierungs- und Automatisierungsgrad lassen sich Workflows voneinander abgrenzen. Die folgende Abbildung zeigt die Unterteilung von Workflows nach dem Strukturierungsgrad.

[18] Vgl. Gierhake, O.(2000), S. 66
[19] Vgl. WfMC (o. J.)
[20] Vgl. Gadatsch, A. (2001), S. 31

Workflow

Allgemeiner Workflow

- vollständig strukturierbare Arbeitsabläufe
- Viele Prozessschritte besitzen einen repetitiven Charakter
- Keine Freiheitsgrade für den Bearbeiter hinsichtlich der Ablaufsteuerung
- Arbeitsschritte im Voraus definierbar

Fallbezogener Workflow

- nicht vollständig strukturierbare Arbeitsabläufe
- Teilweise Prozess-schritte mit repetitiven Charakter
- Freiheitsgrade für den Bearbeiter hin-sichtlich der Ablauf-steuerung
- Arbeitsschritte teilweise im voraus definierbar

Ad hoc Workflow

- nicht strukturierbare Arbeitsabläufe
- Nur wenige Prozess-schritte besitzen einen repetitiven Charakter
- Sehr hohe Freiheits-grade für den Bearbeiter hinsichtlich der Ablaufsteuerung
- Arbeitsschritte nicht im voraus definierbar

Abb. 5: Workflows nach dem Strukturierungsgrad[21]

Wie aus der Abbildung 5 zu entnehmen ist, besitzt der **allgemeine Workflow** den höchsten Strukturierungsgrad. Bedingt durch den hohen Anteil iterativ durchlaufener Elemente und die im Voraus definierbaren Arbeitsschritte eignet sich der allgemeine Workflow optimal zur Unterstützung durch Informationsverarbeitungssysteme. Zusätzlich lässt sich bei der technischen Realisierung ein hoher Grad der Automatisierung erreichen.

Der **fallbezogene Workflow** ist durch einen flexiblen Arbeitsablauf gekennzeichnet. Er enthält teilweise Abschnitte, die iterativ durchlaufen werden und sich somit zur Automatisierung eignen. Die Übergänge zwischen dem fallbezogenen und dem allgemeinen Workflow sind fließend. Gegenüber dem allgemeinen enthält der fallbezogene Workflow höhere Freiheitsgrade für die Bearbeiter der Arbeitsschritte des Workflows.[22]

Im Vergleich zum allgemeinen oder fallbezogenen Workflow ist der Ablauf eines **Ad hoc Workflows** nicht strukturierbar, weshalb eine Modellierung oder gar Automatisierung unmöglich wird. So kann es bei einem Ad hoc Workflow beispielsweise passieren, dass der Bearbeiter erst während der Ausführung einer Aktivität den nachfolgenden Bearbeiter bestimmen kann. Ein solcher Prozess ist für die Abbildung in einem Workflow-Management-System nicht geeignet.

[21] Mit Änderungen entnommen aus: Gadatsch, A. (2010), S. 50
[22] Vgl. Gadatsch, A. (2001), S. 32

Bereits in Kapitel 2.1.2 wurde das Ziel der Automatisierung eines Prozesses durch das Anwenden von Workflow-Management deutlich. Ein Workflow lässt sich somit auch nach dem Grad der möglichen Computerunterstützung unterteilen.

Abb. 6: Workflows nach dem Automatisierungsgrad

Wie aus der Abbildung 6 zu entnehmen ist, wird der **freie** Workflow vollständig manuell durch einen Mitarbeiter bearbeitet. Der **teilautomatisierte** Workflow enthält sowohl Elemente, die maschinell durch eine Workflow-Engine bearbeitet werden können, als auch Aktivitäten, die die Bearbeitung eines qualifizierten Mitarbeiters fordern. Ein Prozess, dessen gesamte Durchführung und Bearbeitung ein Programm übernimmt, wird auch **automatisierter** Workflow genannt.

Für die Automatisierung einer Aktivität muss innerhalb des Workflow-Management-Systems ein Programm durchlaufen werden, welches die Reihenfolge der einzelnen Bearbeitungsschritte festlegt. „Aufgrund dieses Programmes besitzt das [Workflow-Management-]System die Fähigkeit, Entscheidungen zwischen Alternativen des weiteren Ablaufs zu treffen.“[23] Voraussetzung für die Automatisierung ist eine präzise und eindeutige Beschreibung des Ablaufs[24], die, wie in Kapitel 2.1.1 beschrieben, bereits durch das Geschäftsprozessmanagement vorliegt.

Den Großteil der Automatisierungsaufgaben übernimmt die **Workflow-Engine**. Sie „ist die Softwarekomponente, die die Laufzeitunterstützung für die Ausführung des Workflow-Prozesses zur Verfügung stellt. Diese Komponente generiert [**Workflow-]Instanzen**, also Prozesse, aus den zur Verfügung stehenden Prozessmodellen.“[25] Die Engine übernimmt die Aufgaben zur Navigation und Steuerung der einzelnen Aktivitäten, somit auch die Verteilung der Aufgaben an die einzelnen Ressourcen. Administration, Überwachung und Interaktionen mit dem Endanwender gehören auch zu ihren Aufgaben.

Im weiteren Verlauf der Arbeit wird der Fokus, wie in Abbildung 5 und 6 rot markiert, auf einem fallbezogenen Workflow mit einem mittleren Automatisierungsgrad liegen. In den vorhe-

[23] Bretschi, J.(1979), S. 14
[24] Vgl. Freund, J./Götzer, K. (2008), S. 7
[25] Richter-von Hagen, C./Stucky, W. (2004), S. 162

rigen Kapiteln sind die theoretischen Grundlagen für das Erstellen und Verwalten eines Workflows erarbeitet worden. Um praktisch einen fallbezogenen, automatisierten Workflow in einer Engine zu verwalten, muss zuvor noch eine Sprache zur Dokumentation des Prozesses und ein Tool zur Realisierung gewählt werden. Auf die geeignete Vorgehensweise für diese Auswahl der Modellierungssprache und des Tools wird im folgenden Kapitel eingegangen.

2.2 Workflowmodellierungssprachen

Die aktuelle Marktsituation ist gekennzeichnet durch eine große Anzahl an unterschiedlichen Modellierungsmethoden.[26] Die angebotenen Methoden reichen von grafischen Sprachen, über Import-Schnittstellen auf Basis der Extensible Markup Language (XML), bis hin zu tabellarischen Prozessdarstellungen.[27]

2.2.1 BPEL

Die Web Service Business Process Execution Language (WS-BPEL oder BPEL) ist eine Prozessdefinitionssprache, die zur Komposition von Webservices genutzt werden kann, um mächtigere Services zu erhalten.[28] BPEL ist eine XML-basierte Sprache, d.h. die Modellierung eines Workflows entspricht dem Schreiben eines Programmes und kann daher nur mit den nötigen Kenntnissen gelesen und geschrieben werden. Das Arbeiten mit BPEL ist durch die Nutzung von Elementen, wie Schleifen und Bedingungen, weitestgehend blockorientiert. Aufgrund dieser Blockorientierung erhält BPEL eine starre Struktur und unterstützt nur in geringem Maße die Abbildung fachlicher Abhängigkeiten in einem Prozess.[29] Durch diese Gegebenheit ist die Wahrscheinlichkeit von Modellierungsfehlern gering, da die Syntax von BPEL nur erlaubte Funktion zulässt.

Die folgende Tabelle 1 fasst die genannten Vor- und Nachteile von BPEL zusammen.

BPEL	
Vorteile	**Nachteile**
• akzeptierter, verbreiteter Standard • wenig Widersprüche bei der Modellierung möglich • kostenlose Engines sind vorhanden	• der BPEL-Standard enthält keine Symboldefinition • nur für IT-Spezialisten verständlich aufgrund des benötigten Wissens über XML-Notation • aufgrund der Blockorientierung ist die Abbildung fachlicher Abhängigkeiten nicht möglich • starre Ablaufstruktur

Tab. 1: Vor- und Nachteile der Modellierungssprache BPEL

[26] Vgl. Vossen, G./Becker, J. (1996), S. 279
[27] Vgl. zur Mühlen, M./ Hansmann, H. (2008), S. 376
[28] Vgl. Rempp, G. (2011), S. 49
[29] Vgl. Freund, J./Rücker, B. (2012), S. 237

2.2.2 BPMN

Im Gegensatz zu BPEL ist die Business Process Model and Notation (BPMN) keine reine Programmiersprache, sondern der User kann BPMN auch als grafische Modellierungssprache nutzen. Dies hat den Vorteil, dass einerseits die Bedienung durch Symbole einfacher ist und andererseits können bestimmte Funktionalitäten zusätzlich im XML-Dokument programmiert werden. Da BPMN die Modellierung und die Ausführung in der Engine realisiert, ist sie unabhängig von anderen Tools. Seit der neusten Version BPMN 2.0 wird die Beschreibung manuell ausgeführter Aktivitäten besser unterstützt. Aus diesem Grund wird BPMN für die Modellierung des praktischen Teils dieser Arbeit genommen, da der zu modellierende Beispielprozess ein teilautomatisierter, fallbezogener Workflow ist. Ein weiterer wichtiger Grund ist allerdings die einfache Bedienung, da so auch Mitarbeiter ohne spezifische Fachkenntnisse Prozesse modellieren können. Tabelle 2 zeigt eine Zusammenfassung der Vor- und Nachteile von BPMN.

BPMN	
Vorteile	**Nachteile**
• standardisierte, grafische Prozessnotation ermöglicht einfache Bedienung • unabhängig von anderen Tools durch direkte Ausführung in der Workflow-Engine • leicht verständlich • fachliche Abhängigkeiten gut durch die BPMN-Notation abbildbar • kostenlose Engines sind vorhanden • Beschreibung der manuell ausgeführten Aktivitäten wird besser unterstützt • zusätzlich ist die Bearbeitung über ein XML möglich	• allein die Kenntnis der Symbole reicht nicht aus; widersprüchliche Modellierung ist möglich • Gotos sind möglich

Tab. 2: Vor- und Nachteile der Modellierungssprache BPMN

Im Folgenden wird zur Modellierung eines Beispielprozesses in der BPMN-Notation das Workflow-Management-System camunda eingesetzt.

3 Das Workflow-Management-System camunda

Die Software camunda ist ein Workflow-Management-System der Firma camunda Services GmbH. Die camunda Services GmbH entstand durch ein Team von Entwicklern, das sich aus Entwicklern der Community der OpenSource Workflowmanagement-Software Activiti zusammensetzt.

3.1 Einführung in das Tool camunda

Mit Hilfe der Software camunda können Workflows erstellt, verwaltet und überwacht werden. Das Tool existiert in zwei verschiedenen Versionen. Zum einen gibt es eine Community-Version, welche kostenlos eingesetzt werden kann. Sie umfasst das Eclipse-Plugin (ähnlich einem Add-On), mit welchem in der Entwicklungsumgebung Eclipse Workflows in BPMN erstellt werden können. Zum anderen gibt es die Enterprise-Version, die neben den schon genannten Bestandteilen noch Support und zeitnahe Patches umfasst.[30] Durch die Patches wird die Software auf den neusten Stand gebracht sowie neue Funktionalitäten mitgeliefert. Die Kosten des Supports richten sich nach dem gewählten Paket und werden individuell berechnet. Der Support der Enterprise Edition muss für mindestens ein Jahr erworben werden.

3.1.1 Die Installation von camunda

Die Community-Version kann auf der Homepage www.camunda.org heruntergeladen werden. Ein für das Deployen der Workflows notwendiger Webserver lässt sich ebenfalls auf der Website finden. Bei dem Webserver besteht die Wahl zwischen den Produkten Apache Tomcat, JBoss AS7 sowie Glassfish. Innerhalb dieses Projektes wurde der Apache Tomcat 7 eingesetzt. Nach dem Download der beiden Pakete werden diese in ein Verzeichnis der Wahl entpackt. Um den Webserver auf Lauffähigkeit zu testen empfiehlt es sich, die Datei start-camunda.bat im Ordner des Webservers auszuführen. Anschließend sollte sich der Standardbrowser öffnen und die camunda-Startseite erscheinen.

[30] Vgl. Camunda Enterprise (o. J.)

Abb. 7: Die camunda-Startseite

Auf dieser Startseite kann zwischen den Webapplikationen Tasklist, Cockpit und Cycle ausgewählt werden.

3.1.2 Die Bestandteile von camunda

Das **Cockpit** ist eine Web-Applikation, um die laufenden Prozesse zu verwalten und zu überwachen. Es gibt einen Überblick über die verschiedenen Instanzen sowie deren Stati.[31]

Abb. 8: Die Startseite des Cockpits

Im unteren Bereich des Cockpits können die bereits deployten (auf dem Server veröffentlichten) Prozesse betrachtet werden. Nach einem auf einen der Prozesse, öffnet sich eine Detailansicht. Diese Ansicht liefert Informationen darüber, an welchem Punkt sich der Prozess aktuell befindet und wie viele Instanzen existieren.

[31] Vgl. Camunda Features (o. J.)

Abb. 9: Aktueller Standpunkt des Prozesses

Um eine Aufgabe zu bearbeiten bzw. zu beenden, muss die Perspektive von Cockpit auf Tasklist gewechselt werden. Die **Tasklist** ist eine Web-Applikation, die die auszuführenden Aufgaben eines Nutzers anzeigt. Angezeigt werden der Name der Aufgabe, der Prozessname und das Startdatum. Hier besteht die Möglichkeit, einen Task auszuführen oder abzubrechen. Mit **Cycle** können Modelle verschiedener Tools miteinander synchronisiert werden.[32] Zum Beispiel die Synchronisation von Modellen, die mit dem Signavio Modeler erstellt wurden mit einem von camunda erstellten Modell.

Den genannten drei Webapplikationen werden die Daten durch verschiedene Interfaces der Process Engine bereitgestellt. Folgende Abbildung zeigt die acht verfügbaren Interfaces der Java-API.

Abb. 10: Die Process-Engine-API[33]

Auf dieser Process-Engine-API basieren alle von camunda bereitgestellten Funktionalitäten. Diese werden in der folgenden Tabelle erläutert:[34]

Bestandteil	Erläuterung
RepositoryService	Der RepositoryService enthält Methoden, um Deloyments und Prozesse zu verwalten bzw. abzuändern. Er unterstützt das Deployen von Prozessen und enthält statische Initialisierungsdaten.
TaskService	Der TaskService ist für die Verwaltung der einzelnen Tasks zuständig. Unter anderem weist er Aufgaben Usergruppen bzw. dem einzelnen User zu und speichert den Bearbeitungsstatus.
IdentityService	Der IdentityService führt Userverwaltungsaktionen durch. Dazu ge-

[32] Vgl. Camunda Cycle (2013)

[33] Enthalten in: Camunda Docs (2013)

[34] Vgl. Camunda Docs (2013)

	hört das Verwalten von Neuanlagen, Gruppenänderungen sowie das Löschen von Nutzern. Die Engine überprüft nicht, ob der Nutzer, dem die Aufgabe zugewiesen ist, tatsächlich existiert.
FormService	Mit dem FormService können grafische Masken angelegt werden, die der User vor dem Prozessstart und vor dem Abschließen einer Task angezeigt bekommt.
AuthorizationService	Dieser Service ist verantwortlich für das Zuweisen und Verwalten von Rechten bei bestimmten Nutzern bzw. kompletten Nutzergruppen.
RuntimeService	Der RuntimeService ist für die Initialisierung neuer Prozessinstanzen zuständig. Er verwaltet alle laufenden Instanzen bzw. speichert deren aktuellen Stand und die Belegung verschiedener Variablen.
ManagementService	Der ManagementService stellt Informationen über Datenbanken und Metadaten-Datenbanken bereit. Zusätzlich enthält er Funktionen für Administratoren und Instandhaltungsarbeiten.
HistoryService	Der HistoryService zeichnet Daten (z.B. Startzeit, Bearbeiter, Dauer) zu einem Prozess während der Laufzeit auf und speichert diese in einer Datenbank ab. Die abgelegten Daten auch nach Prozessende in der Datenbank hinterlegt und können durch Methoden abgerufen sowie weiterverwendet werden.

Tab. 3: Interfaces der Java API

3.1.3 Anlegen eines Projekts

Grundsätzlich basiert jeder Prozess auf der XML, die ein strukturiertes, nach sogenannten Tags gestaffeltes Dokumentenformat beschreibt.[35] Der camunda Modeler bietet die grafische Oberfläche zur Modifikation dieser XML-Dateien. Der Weg des manuellen Anpassens des XMLs bleibt dem Nutzer mit entsprechenden Editoren zusätzlich bestehen.

Im **Modeler** können folgende **BPMN-Elemente** verwendet werden, um Workflow-Modelle zu erstellen: [36]

Grafiken	Erläuterung
	Das Start-Element kennzeichnet den Beginn eines Workflows.
	Das Ende-Element kennzeichnet das Ende eines Workflows, wobei mehrere existieren können.
	Eine User-Task beschreibt eine Arbeitseinheit für einen Prozessbeteiligten.

[35] Vgl. Eckstein, R. / Casabianca, M. (2002), S. 5

[36] Vgl. Camunda Reference (2013)

	Mit Hilfe des Sequence-Flows werden verschiedenen Modellierungselemente zu einem Workflow verbunden und bestimmt somit die Abfolge der Ausführung.
	Die Call-Activity kann global definierte Teilprozesse über deren Process-ID zur Laufzeit aufrufen. Zu erkennen ist die Call-Activity an ihrem dicken, schwarzen Rahmen.
	Das Parallel-Gateway kennzeichnet den Beginn und das Ende parallel ausgeführter Tasks. Bei einer Verzweigung werden alle ausgehenden Sequence-Flows aktiviert. Bei der Zusammenführung müssen alle eingehenden Aktivitäten bearbeitet sein, bevor der Workflow fortfahren kann.
	Dieses exlusive Gateway stellt eine Verzweigung mit Bedingung dar. Abhängig von der Bedingung wird eine der Ausgangsaktivitäten aktiviert. Werden verschiedene Aktivitäten bei diesem Element zusammengeführt, wird auf die Aktivität gewartet, die die Bedingung erfüllt. Ist diese Eingangsbedingung erfüllt, wird der Workflow fortgesetzt.
	Es gibt verschiedene Event-Typen: Bei einem **Throw-Event** wird ein Ereignis ausgelöst, das sich auf ein Ziel außerhalb des Workflows bezieht. Bei einem MessageThrow erfolgt zum Beispiel ein E-Mail-Versand an eine bestimmte Mail-Adresse. **Catch-Events** sind vielseitig einsetzbar. So kann es unter anderem als Timer (z.B. als Stoppuhr) oder als Mail-Trigger für den Mailversand dienen. **Boundary-Events** sind im Gegensatz zu den oben genannten Events an einen Task angefügt. Sie können u.a. die gleichen Aufgaben wie Throw- und Catch-Events übernehmen. **Timer-gesteuerte Events** laufen abhängig von einer einstellten Zeit. Z.B. können Tasks zu einer bestimmten Zeit gestartet werden.
	Ein Pool umfasst den gesamten Prozess. Dabei kann ein Pool sowohl eine Organisation, eine Rolle oder ein System darstellen.
	Lanes werden eingesetzt, um einen Pool feiner zu unterteilen. Damit können verschiedene Verantwortlichkeiten innerhalb einer Organisation oder eines Systems getrennt dargestellt werden.

Tab. 4: Überblick über die grundlegenden BPMN-Elemente

3.1.4 Das Anlegen eines Beispielmodells

Um einen Prozess anzulegen, folgt man den Schritten der Anleitung unter folgendem Link: http://camunda.org/get-started/developing-process-applications.html.

In diesem Teil der Arbeit wird beschrieben, an welchen Punkten der Anleitung bezüglich der Prozesserstellung weitere Details zu beachten sind, da sich die Einrichtung auf den Testrechnern punktuell als sehr mühsam herausgestellt hat.
Der erste Tipp betrifft die XML-Datei pom.xml. Anstatt hier die Tags nach den in der Anleitung markierten Stellen zu durchsuchen, sollte man sich den Inhalt der pom.xml von der Website aus dem Beispiel ab den Tag <dependencies> kopieren. Neben dem Sparen von Zeit wird so auch eine Fehlerquelle ausgeschlossen.
Der nächste Hinweis betrifft die Datei processes.xml, die in den neu hinzugefügten Ordner META-INF zu erstellen ist. Innerhalb des Tags <properties> existiert ein Eintrag isDeleteUponUndeploy. Setzt man den Wert von false auf true, wird die alte Version des Prozesses automatisch undeployed (vom Sever gelöscht), sobald eine neue Version darauf deployed (veröffentlicht) wird.
Bei der zu erstellenden User-Task sollte statt dem normalen User john der Testadmin demo eingegeben werden. Das bietet den Vorteil, dass während eines späteren Tests des Prozesses auch Administratorelemete (z.B. den Prozess vorzeitig beenden, an andere User übergeben, usw.) verwendet werden können.
Beim Schritt der Erstellung der war-Datei, die später auf dem Server deployed wird, kann anstatt der pom.xml auch der gesamte Maven-Projekt-Ordner markiert und als Maven Install ausgeführt werden. Bei beiden Verfahren entsteht die gewünschte war-Datei.
Das Ende der grundsätzlichen Testprozesserstellung endet an der Stelle mit camunda Cockpit. Sollte der Prozess bei den ersten Versuchen des Deployens Fehler verursachen, sollte die Log-Datei auf etwaige Fehlermeldungen überprüft werden.

3.2 Benutzerverwaltung

Prozessmanagement setzt ein klar definiertes Rollenmodell voraus, damit Verantwortlichkeiten und Aufgaben der Prozessbeteiligten festgelegt sind.[37] Prozessbeteiligte, auch Akteure genannt, können durch ihre Kompetenzen die gleiche Rolle haben.[38] So kann in einer Rolle definiert werden, welche Aufgaben und Verantwortlichkeiten die Personengruppe hat, die die Rolle besitzt. Durch die Definition von Rollen lassen sich auch die Rechte ableiten, die für bestimmte Aktivitäten oder Zugriffe auf das Workflow-Management-System erforderlich sind. Je nach Bedarf können unterschiedliche Management-Rollen festgelegt werden, die für die Durchführung des Prozesses notwendig sind. Neben den Management-Rollen, gibt es die Ausführungsverantwortlichen, die innerhalb des Prozesses eine bestimmte Aufgabe zu erle-

[37] Vgl. BPM Akademie (o.J.)
[38] Vgl. Richter-von-Hagen, C. / Stucky, W. (2004), S. 35

digen haben.[39] Da die definierten Rollen in jedem Unternehmen variieren, werden im Folgenden nur die Rollen beschrieben, die für den Beispielprozess relevant sind.

In dem bereits erläuterten Beispielprozess Softwareverteilung, gibt es die Management-Rolle Admin. Aus Gründen der Verständlichkeit fällt die Rolle des Rollout-Verantwortlichen mit der des Administrators zusammen. Er ist für die strategische Planung, Ausführung und Steuerung des Prozesses zuständig. Auch die für die Prozesssteuerung und Prozessausführung benötigten Ressourcen werden von ihm koordiniert.[40] Im Beispielprozess ist der Admin gleichzeitig Prozessbeteiligter, weil er gewisse Tasks ausführt.

Die Rolle IT ist für die Ausführung bestimmter Tasks zuständig und ist somit Prozessbeteiligter. Die Ausführung des Prozesses ist Teil seiner täglichen Arbeit. Treten bei der Durchführung des Prozesses Fehler auf, werden diese an den Admin gemeldet.

Eine andere Rolle bilden die Tester, die ebenfalls bestimmte Tasks innerhalb des Prozesses ausführen.

Um das definierte Rollenmodell für den Prozess umzusetzen, bietet camunda zwei Möglichkeiten. Diese sind zum einen die Services Identity Service und Authorization Service, die die camunda Engine API bietet. Zum anderen kann über das Anwendungsprotokoll Lightweight Directory Access Protocol (LDAP) auf die Benutzer und Rechte des Verzeichnisdienstes des Unternehmens zugegriffen werden. In den nächsten beiden Unterkapiteln werden beide Möglichkeiten der Benutzerverwaltung näher dargestellt.

3.2.1 Identity Service und Authorization Service

Eine der Kernschnittstellen der camunda Engine API ist der Identity Service.[41] Dieser erlaubt das Verwalten von Benutzer und Gruppen. Der Identity Service verwendet dabei standardmäßig die Datenbank der Process Engine für die Benutzerverwaltung, wenn keine alternative Implementierung zur Benutzerverwaltung zur Verfügung steht. Dabei unterscheidet camunda folgende drei Entitäten:

Benutzer

Benutzer können im camunda Cockpit mit einer eindeutigen Benutzer-ID, einem Passwort, sowie dem Vor- und Nachnamen und der E-Mailadresse angelegt werden.

[39] Vgl. Konsequent (o.J.)
[40] Vgl. BPM Akademie (o.J.)
[41] Vgl. Rademakers, T. (2012)

Abb. 11: Benutzer anlegen

Die Übersicht über alle angelegten Benutzer im camunda Admin Tool sieht wie folgt aus.

Abb. 12: Angelegte Benutzer

Sind die Benutzer angelegt, müssen die Rollen in camunda abgebildet werden. Das Rollenmodell kann umgesetzt werden, in dem alle Mitarbeiter mit der gleichen Rolle einer Gruppe zugeordnet werden. Die zugehörigen Rechte der Rollen werden an die Gruppen vergeben, sodass alle Gruppenmitglieder die Rechte bekommen. So müssen die Rechte nicht den einzelnen Benutzer vergeben werden, sondern werden an die Gruppen vergeben und die Benutzer werden der Gruppe hinzugefügt. So macht es Sinn, für die verschiedenen Rollen (Admin, IT und Tester) Gruppen anzulegen.

Gruppen

Gruppen werden mit einer eindeutigen Gruppen-ID, einem Namen und dem Typen angelegt (siehe Abbildung 13).

Abb. 13: Gruppe anlegen

Bei dem Gruppentyp wird unterschieden zwischen WORKFLOW und SYSTEM. Der Typ WORKFLOW ist geeignet für eine Gruppe, deren Mitglieder Prozessbeteiligte sind. Der Typ SYSTEM ist eher für die Administratorengruppe geeignet. So wurden Gruppen mit folgenden Typen angelegt.

Groups

Group Id	Group Name	Group Type	
admingruppe	Admin-Gruppe	SYSTEM	Edit
itgruppe	IT-Gruppe	WORKFLOW	Edit
testergruppe	Tester-Gruppe	WORKFLOW	Edit

Abb. 14: Angelegte Gruppen

Zugehörigkeit

Nachdem die Gruppen und Benutzer angelegt sind, müssen die Zugehörigkeiten zwischen diesen durch Mitgliedschaften hergestellt werden. Dies ist durch das Hinzufügen einer Gruppe in das Profil des Benutzers möglich.

Abb. 15: Gruppe in das Profil hinzufügen

Zusammengefasst sind folgende Benutzer und Gruppen angelegt.

Gruppen-ID	Gruppenname	Gruppentyp
admingruppe	Admin-Gruppe	SYSTEM
testergruppe	Tester-Gruppe	WORKFLOW
itgruppe	IT-Gruppe	WORKFLOW

Tab. 5: Angelegte Gruppen

User-ID	Name	Passwort	Gruppenzugehörigkeit
admin	Adrian Admiral	********	admingruppe
tester	Thomas Tapfer	********	testergruppe
it	Iris Imker	********	itgruppe

Tab. 6: Benutzer

Um nun Berechtigungen auf bestimmte Ressourcen vergeben zu können, kommt der Authorization Service zum Einsatz. Camunda unterstützt ein Framework für eine ressourcenorientierte Zugriffsverwaltung.[42] Somit können einer Identität Berechtigungen für Ressourcen erteilt werden. Folgende Abbildung zeigt diesen Zusammenhang der drei Elemente.

Abb. 16: Zusammenhang von Benutzer, Berechtigung und Ressource

Bei den Identitäten wird unterschieden zwischen einem bestimmten Benutzer, allen Benutzern und einer Gruppe. Einem Benutzer kann eine Berechtigung direkt oder über die zugehörige Gruppe zugewiesen werden. Berechtigungen hingegen beschreiben, in welcher Form die Identität mit der Ressource interagieren darf. Diese sind CREATE, READ, UPDATE und DELETE. Weitere Berechtigungen können individuell eingebaut werden.[43] Ressourcen sind die Entitäten, mit denen der Benutzer interagieren darf.[44] Das camunda BPM Framework unterstützt folgende Ressourcen:

- Applikationen (z.B. Cockpit, Tasklist, Admin)
- Autorisierungen
- Gruppen

[42] Vgl. Camunda Docs (2013)
[43] Vgl. Camunda Docs (2013)
[44] Vgl. Camunda Docs (2013)

- Gruppenzugehörigkeit
- Benutzer

Damit die Benutzer z.B. ihre Tasklist sehen können, müssen die Berechtigungen dieser Applikation vergeben werden (siehe folgende Abbildung).

RESOURCES
Application
Authorization
Group
Group Membership
User

Application Authorizations

Type	User / Group	Permissions	Resource Id	Action
ALLOW	admingruppe	ALL	*	delete
ALLOW	itgruppe	ACCESS	*	delete
ALLOW	testergruppe	ACCESS	*	delete
ALLOW	Group User / Group Id	ALL	* (cockpit or tasklist or *)	

Abb. 17: Berechtigung für Applikationen

Darüber hinaus können kundenspezifische Ressourcen wie z.B. Prozess-Instanzen und Tasks definiert werden.[45]

Mit all diesen Funktionen bietet camunda eine simple Benutzerverwaltung, was sich jedoch für den Einsatz im Unternehmen nur bedingt eignet. Für Unternehmen ist es wichtig, dass diese die Benutzerverwaltung nur an einer zentralen Stelle durchführen. Deshalb ist die Anbindung des betrieblichen Verzeichnisdienstes sinnvoll, um mehrfache Benutzerverwaltungen zu vermeiden.

3.2.2 LDAP Identity Service

Standardmäßig verwendet die Engine den Identity Service für die Benutzerverwaltung, welcher die Benutzer in der Engine-Datenbank ablegt. In der Praxis verwenden große Unternehmen jedoch Verzeichnisdienste, um die große Menge an Benutzer und andere Ressourcen zentral verwalten zu können. So dient ein LDAP-Server meistens als Lösung für die Benutzerverwaltung.[46] Der LDAP Identity Service ermöglicht den Zugriff auf die Daten eines Verzeichnisdienstes. Diese Möglichkeit bietet gegenüber der Userverwaltung mit dem Identity Service der Engine den Vorteil, dass die Benutzer sowie alle Rechte nur an einer zentralen Stelle verwaltet werden, was Dateninkonsistenzen vermeidet.[47]
Um den LDAP Identity Service verwenden zu können, muss zunächst die camunda-identity-ldap.jar Bibliothek in den Klassenlader aufgenommen werden. Dies erfolgt durch das Hinzufügen eines Dependency-Tags in die pom.xml Datei (siehe Abbildung 18).[48]

[45] Vgl. Camunda Docs (2013)
[46] Rademakers, T. (2012), S. 236
[47] Vgl. Hetze, S. (2002)
[48] Vgl. Camunda Docs (2013)

```
<dependency>
  <groupId>org.camunda.bpm.identity</groupId>
  <artifactId>camunda-identity-ldap</artifactId>
  <version>${camunda.version}</version>
</dependency>
```

Abb. 18: Dependency hinzufügen

Doch die eigentliche Konfiguration des LDAP Identity Provider Plugins findet in der Konfigdatei bpm-platform.xml statt. Dazu muss die Datei mit folgendem Plugin-Tag erweitert werden.

```
<plugins>
  <plugin>
    <class>org.camunda.bpm.identity.impl.ldap.plugin.LdapIdentityProviderPlugin</class>
    <properties>

      <property name="serverUrl">ldap://localhost:4334/</property>
      <property name="managerDn">uid=jonny,ou=office-berlin,o=camunda,c=org</property>
      <property name="managerPassword">s3cr3t</property>

      <property name="baseDn">o=camunda,c=org</property>

      <property name="userSearchBase"></property>
      <property name="userSearchFilter">(objectclass=person)</property>

      <property name="userIdAttribute">uid</property>
      <property name="userFirstnameAttribute">cn</property>
      <property name="userLastnameAttribute">sn</property>
      <property name="userEmailAttribute">mail</property>
      <property name="userPasswordAttribute">userpassword</property>

      <property name="groupSearchBase"></property>
      <property name="groupSearchFilter">(objectclass=groupOfNames)</property>
      <property name="groupIdAttribute">ou</property>
      <property name="groupNameAttribute">cn</property>

      <property name="groupMemberAttribute">member</property>

    </properties>
  </plugin>
```

Abb. 19: LDAP Identity Provider Plugin[49]

Die Abbildung 19 enthält die notwendigen Properties mit beispielhaften Werten. Genaueres zu den einzelnen Properties liefert folgende Tabelle 7.

Eigenschaft	Beschreibung
serverUrl	Die Uniform Resource Locator (URL) des LDAP Servers
managerDn	Der Distinguished Name (DN) des Managers des Verzeichnisdienstes (dessen Nutzerdaten für den Zugang verwendet werden)
managerPassword	Das Passwort des Managers
baseDn	Der DN des Einstiegspunktes für die Suche

[49] Enthalten in Camunda Docs (2013)

userSearchBase	Der Knoten innerhalb des LDAP-Baumes, ab wo die Suche nach Benutzer starten soll
userSearchFilter	LDAP-Abfrage, die bei der Benutzersuche verwendet werden soll
userIdAttribute	Der Name für die Benutzer-ID-Property
userFirstnameAttribute	Der Name für die Vornamen-Property
userLastnameAttribute	Der Name für die Nachnamen-Property
userEmailAttribute	Der Name für die E-Mail-Property
userPasswordAttribute	Der Name für die Passwort-Property
groupSearchBase	Der Knoten innerhalb des LDAP-Baumes, ab wo die Suche nach Gruppen starten soll
groupSearchFilter	LDAP-Abfrage, die bei der Gruppensuche verwendet werden soll
groupIdAttribute	Der Name für die Gruppen-ID-Property
groupNameAttribute	Der Name für die Gruppennamen-Property
groupTypeAttribute	Der Name für die Gruppen-Typ-Property
groupMemberAttribute	Der Name für die Mitgliedschaftsproperty
acceptUntrustedCertifiicates	Akzeptanz von nicht vertrauenswürdigen Zertifikaten bei der Verwendung von SSL
useSsl	Verwendung von Secure Socket Layer (SSL) für die LDAP Verbindung
initialContextFactory	Der Wert für die java.naming.factor.initial-Property
securityAuthentication	Der Wert für die java.naming.security.authentication-Property

Tab. 7: Properties des LDAP Identity Provider Plugins[50]

Das LDAP Identity Provider Plugin wird meistens zusammen mit dem Administrator Authorization Plugin verwendet. Das Administrator Authorization Plugin ermöglicht die Erteilung von der Administrationsvollmacht an einen LDAP-Benutzer oder einer LDAP-Gruppe.[51] Bei der Auslieferung von camunda BPM wird durch das Invoice-Beispiel ein Benutzer namens demo erstellt, der die Administrationsvollmacht erteilt bekommt. Auch die Webapplikation Admin ermöglicht beim ersten Aufruf das Anlegen eines Ausgangsadminstrators, wenn in der Datenbank kein Benutzer angelegt ist. Dies ist jedoch beim LDAP Identity Service nicht der Fall, weil dieser nur einen lesenden Zugriff auf das Benutzerverzeichnis hat, sodass das Anlegen eines Ausgangsadministrators nicht möglich ist. So muss das Adminstrator Authorization Plugin eingesetzt werden, um einem LDAP-Benutzer oder einer LDAP-Gruppe die Administratorberechtigungen zu vergeben. Dies ist durch das Hinzufügen eines Plugin-Tags in die Konfigurationsdatei bpm-platform.xml möglich. Dieses Plugin gewährt dem LDAP-Benutzer

[50] Vgl. Camunda Docs (2013)
[51] Vgl. Camunda Docs (2013)

alle Berechtigungen auf alle Ressourcen. Folgende Abbildung zeigt einen beispielhaften Plugin-Tag.

```
<process-engine name="default">
  ...
  <plugins>
    <plugin>
      <class>org.camunda.bpm.engine.impl.plugin.AdministratorAuthorizationPlugin</class>
      <properties>
        <property name="administratorUserName">admin</property>
      </properties>
    </plugin>
  </plugins>
</process-engine>
```

Abb. 20: Administrator Authorization Plugin

Die einzugebende Properties sind Folgende.

Eigenschaft	Beschreibung
administratorUserName	Der Name des Administrator-Benutzers
administratorGroupName	Der Name der Administrator-Gruppe

Tab. 8: Properties des Administrator Authorization Plugins

4 Modellieren eines Prozesses mit dem Worflow-Management-System camunda

Das folgende Kapitel beschreibt die Modellierung und Implementierung eines Beispielprozesses mit dem Workflow-Management-System camunda. Da der Beispielprozess alle typischen Anforderungen an einen Workflow enthält, können die dargelegten Konzepte auf alle ähnlichen Prozesse übertragen werden.

4.1 Prozessbeispiel Softwareverteilung

In großen Unternehmen ist die Vorbereitung und Ausführung der Installation neuer Software ein aufwendiger und komplexer Prozess. Da Mitarbeiter dieser Unternehmen die Software nicht eigenständig auf ihren Rechnern installieren können, müssen die Aufgaben der Softwareverteilung von der IT-Abteilung durchgeführt werden. Der Prozess, der den Weg der Software von der IT-Abteilung auf den Rechner des Mitarbeiters beschreibt, wird als Softwareverteilung bezeichnet. Bei der Bereitstellung von neuen Softwareversionen für eine große Anzahl von Mitarbeitern, gilt es den Verteilungsprozess genau zu planen.

4.1.1 Gesamtprozess Softwareverteilung

Im Folgenden wird exemplarisch aufgezeigt, wie mit dem Workflow-Management-System camunda der Softwareverteilungsprozess im Unternehmen organisiert werden kann. Der Prozess wurde eigens für diese Demonstration entworfen. An manchen Stellen wird auf eine realistischere Darstellung zu Gunsten der Übersichtlichkeit verzichtet. Ziel der Beschreibung ist die Übertragbarkeit der dargestellten Konzepte auf jegliche praktische Prozesse mit ähnlichen Anforderungen. In dieser Dokumentation wird aufgezeigt, wie die Organisation des Softwareverteilungsprozesses automatisiert werden kann (z.B. automatisierte Aufgabenverteilung durch Versenden einer Informationsmail vor jedem Task). Natürlich bietet die Workflow-Engine Möglichkeiten, um auch die Ausführung von Tasks zu automatisieren. Prinzipiell ist dabei alles möglich, was sich mit der Programmiersprache Java umsetzen lässt, da die Workflow-Engine den Aufruf von Java-Klassen erlaubt. Die Automatisierung von Tasks ist jedoch sehr individuell und zunächst einmal unabhängig von camunda. Deshalb wurde in der vorliegenden Dokumentation oft auf die Beschreibung dieser Form der Automatisierung verzichtet.
Abbildung 21 stellt den in der Dokumentation implementierten Gesamtprozess „Softwareverteilung“ in der BPMN-Notation dar.

Abb. 21: Gesamtprozess Softwareverteilung

In der Tabelle 9 werden die einzelnen Tasks des Gesamtprozesses beschrieben.

Task	Beschreibung der Task
1 Usergruppen einteilen	Nicht alle Mitarbeiter des Unternehmens sollen eine neue Softwareversion am gleichen Tag erhalten. Deshalb werden in Task 1 die Anwender in Gruppen aufgeteilt und es wird festgelegt, für welche Gruppe im weiteren Prozess eine Verteilung der Software erfolgt. In camunda Tasklist muss der Bearbeiter die Durchführung der Aufgabe bestätigen. Bearbeiter: **admin**
2 Ankündigungsmail versenden	In Task 2 wird eine Ankündigungsmail erstellt, die anschließend an alle Empfänger des Softwarepakets versendet wird. In dieser Mail werden die Mitarbeiter gebeten am Tag der Umstellung ihren Rechner herunterzufahren. Der Bearbeiter der Task füllt in camunda Tasklist ein Formular mit den Werten „Datum der Verteilung" und „Name des Softwarepaketes". Die eingegeben Werte werden dann in das Mailtemplate eingefügt und die Ankündigungsmail wird automatisch versendet. Bearbeiter: **admin**
3 Softwarepaket bereitstellen	Die IT-Abteilung muss bis kurz vor dem Termin der Softwareverteilung aktuelle Anforderungen und Änderungen des Softwarepaketes berücksichtigen. Sobald das Paket vollständig ist, meldet die IT-Abteilung dem Administrator und Rollout-Verantwortlichem dies per Mail. Die Meldung erfolgt in camunda Tasklist. Bearbeiter: **it**
4 Softwarepaket testen	Bevor das Softwarepaket verteilt wird, wird es durch einen Tester überprüft. Das Ergebnis des Tests wird in camunda Tasklist festgehalten. Falls der Tester feststellt, dass noch Fehler vorhanden sind, muss das Softwarepaket nachgebessert werden, wofür die Tasks 3 und 4 wiederholt werden müssen. Hier soll eine Logik implementiert werden, die diese Wiederholung anstößt (Retry). Falls keine Fehler gefunden wurden, kann direkt die nächste Task begonnen werden. Bearbeiter: **tester**
5 Softwarepaket installieren	Task 5 beinhaltet die komplette Installation des Softwarepaketes. Da dies ein komplexer Prozess für die IT-Abteilung ist, soll aus Gründen der Übersichtlichkeit die Aufgaben der Task 5 als Subprozess modelliert werden. In diesem Subprozess ist für jeden Bearbeitungsschritt eine eigene Task vorhanden.
6 Bericht versenden	In Task 6 stößt der Administrator den Versand eines Berichts an. Wenn er diese Task abschließt, wird auch die Instanz des laufenden Prozesses beendet. In dem Bericht finden sich Informationen zum Prozessablauf, sodass dieser als Grundlage für die kontinuierliche Verbesserung des Softwareverteilungsprozesses verwendet werden kann. Bearbeiter: **admin**

Tab. 9: Beschreibung der Tasks des Gesamtprozesses

4.1.2 Subprozess Softwarepaket installieren

Abbildung 22 zeigt den in der BPMN Notation dargestellten Subprozess der die Installation des Softwarepaketes in einzelne Tasks aufgliedert.

Abb. 22: Subprozess Softwarepaket installieren

Die folgende Tabelle 10 enthält die Beschreibung der Tasks des Subprozesses.

Task	Beschreibung der Task
5.1 Ermittlung nicht erreichter Clients	Die IT-Abteilung hat die Aufgabe, die Anzahl und Arbeitsplatznummern der Clients zu ermitteln, die nicht heruntergefahren wurden. Diese konnten nicht mit der neuen Software betankt werden. Eine Ergebnisliste ist an den Administrator zu versenden. Danach wird die Durchführung der Aufgabe in camunda Tasklist bestätigt. Bearbeiter: **it**
5.2 Verteilung des Softwarepaketes	Die Verteilung des Softwarepaketes soll erst zu einer bestimmten Uhrzeit gestartet werden, beispielsweise außerhalb der Kernarbeitszeit. Die IT-Abetilung bestätigt in camunda Tasklist, dass die Verteilung des Softwarepaketes abgeschlossen ist und die Installation daher beginnen kann. Diese Funktionen sollen im modellierten Workflow abgebildet werden. Bearbeiter: **it**
5.3 Installation des Softwarepaketes	Die Installation des Softwarepakets darf eine gewisse Dauer nicht überschreiten, da beispielsweise gewährleistet sein muss, dass die Clients den Mitarbeitern am nächsten Arbeitstag wieder zur Verfügung stehen. Falls die vorgegebene Dauer überschritten wird, muss eine Alarm-Mail an dem Administrator versendet werden. Die Task 5.3 soll dennoch zunächst nicht abgebrochen werden, da vorerst die Benachrichtigung des Administrators als Anforderung genügt. Die IT-Abteilung bestätigt in camunda Tasklist die Beendigung der Installation auf den Clients. Bearbeiter: **it**
5.4 Alarm-Mail an Admin	In Task 5.4 wird eine Alarm-Mail an den Administrator versendet, wenn die Task 5.3 länger dauert als geplant. Diese Task wird automatisch ausgeführt und benötigt daher keinen Bearbeiter. Bearbeiter: **automatischer Versand**

Tab. 10: Beschreibung der Tasks des Subprozesses

4.1.3 Abgeleitete Anforderungen

Aus dem oben beschriebenen Prozess lassen sich die folgenden Einzelanforderungen ablei-ten:

- Verwaltung mehrerer Benutzer in Benutzergruppen mit unterschiedlichen Rechten.
- Mailversand an den Bearbeiter zu Beginn einer Task.
- Funktionalität, die einem Bearbeiter erlaubt, die erfolgreiche Durchführung einer Task zu bestätigen oder Fehler zu melden.
- Abbildung parallel laufender Prozesse mit zeitlichen, fachlichen und technischen Ab-hängigkeiten.
- Retry einzelner Aufgaben: Durch Implementierung alternativer Ablaufszenarien kann gesteuert werden, ob die Durchführung bestimmter Aufgaben wiederholt werden soll.
- Timer-gesteuerter Start einer Task zu einer bestimmten Uhrzeit.
- Alarmfunktion bei Laufzeitüberschreitung (im Vergleich zur geplanten Dauer) einzel-ner Tasks, zum Beispiel durch Versand einer Alarm-Mail an den Verantwortlichen.
- Zusammenfassung zusammengehörender Aufgaben zu Subflows.
- Einbindung einer Konfigurationsdatei, um die Eigenschaften einer Aufgabe flexibel festlegen zu können (zum Beispiel Dauer, Startzeit).
- Protokollierung in einer Log-Datei.
- Ermöglichen eines Replans: Falls bestimmte Aufgaben nicht wie geplant durchlaufen, wird die Flexibilität durch einen Replan erhalten. Dazu wird die aktuelle Ausführung des Prozesses unterbrochen und ein geänderter Prozess modelliert und deployt.

4.2 Implementierung von Basiskonzepten

Im Folgenden wird die Implementierung des Beispielprozesses Softwareverteilung mit dem Workflow-Management-System camunda praxisnah erklärt.

4.2.1 User Task

Um eine Aufgabe zu modellieren, die von einer Person ausgeführt werden soll, benötigt man eine User Task. Abbildung 23 zeigt, einen Prozess mit der User Task „1 Usergruppen eintei-len“, die im Folgenden auch als Task 1 bezeichnet wird.

Abb. 23: Prozess mit einer User Task

Markiert man im Modeler Task 1 und navigiert unter **Properties** zur Kategorie **General**, lassen sich die Eigenschaften einer Task bearbeiten, ohne dazu manuell das Workflow-XML (siehe 3.1.3) verändern zu müssen.

Tasks | Properties | Console | Problems

User Task "1
Usergruppen einteilen"

General
Multi Instance
Listener
Form Fields

Id: UserTask_1
Name: 1
Usergruppen einteilen
Assignee: admin
Candidate Users:
Candidate Groups:
Form Key: embedded:app:forms/ankuendigungsmail.html
Due Date:
Priority:

Abb. 24: Properties der Task 1

Abbildung 24 zeigt, dass unter **Assignee** bereits beim Modellieren ein Bearbeiter für die Aufgabe festgelegt werden kann. Im Beispiel ist das die Person mit der Benutzerkennung admin.

Im Feld **Form Key** wurde ein HTML-Formular mit der Task 1 verknüpft, welches beim Aufruf der Task ausgeführt wird. Dieses Formular kann sowohl Daten anzeigen, als auch Eingabedaten des Bearbeiters abfragen, die dann als Prozessvariablen im weiteren Ablauf verwendet werden können. Bei **Priority** kann die Wichtigkeit der Task durch eine Zahl zwischen 1 und 100 festgelegt werden. Bleibt das Feld wie im Beispiel unausgefüllt, wird automatisch eine Priorität von 50 angenommen.

Im XML ist die Task 1 dann wie in Abbildung 25 erkennbar definiert.

```
<bpmn2:userTask id="UserTask_1" camunda:assignee="admin"
    camunda:formKey="embedded:app:forms/ankuendigungsmail.html"
    name="1&#xD;&#xA;Usergruppen einteilen">
  <bpmn2:incoming>SequenceFlow_1</bpmn2:incoming>
  <bpmn2:outgoing>SequenceFlow_2</bpmn2:outgoing>
</bpmn2:userTask>
```

Abb. 25: XML-Repräsentation Task 1

4.2.2 Parallelität

Sofern Tasks weder fachliche, noch technische oder zeitliche Abhängigkeiten besitzen, bietet es sich an, diese Tasks parallel durchzuführen. Abbildung 26 zeigt, wie eine Parallelität modelliert wird.

Abb. 26: Prozess mit parallel ablaufenden Tasks

Im Beispiel werden Task 2 und Task 3 parallel ausgeführt. Dies bietet sich an, da die Aufgaben keine Abhängigkeiten besitzen und zudem von unterschiedlichen Bearbeitern ausgeführt werden. Im XML werden dazu an den parallelen Gateways jeweils die ein- und ausgehenden Prozessstränge (Sequence Flows) definiert (siehe Abbildung 27).

```
<bpmn2:parallelGateway id="ParallelGateway_1">
  <bpmn2:incoming>SequenceFlow_2</bpmn2:incoming>
  <bpmn2:outgoing>SequenceFlow_3</bpmn2:outgoing>
  <bpmn2:outgoing>SequenceFlow_4</bpmn2:outgoing>
</bpmn2:parallelGateway>
```

```
<bpmn2:parallelGateway id="ParallelGateway_2">
  <bpmn2:incoming>SequenceFlow_5</bpmn2:incoming>
  <bpmn2:incoming>SequenceFlow_6</bpmn2:incoming>
  <bpmn2:outgoing>SequenceFlow_7</bpmn2:outgoing>
</bpmn2:parallelGateway>
```

Abb. 27: XML-Repräsentation der parallelen Gateways

4.2.3 Execution und Task Listener

Execution und Task Listener sorgen für die Ausführung von Java Code an einer vorher definierten Stelle im Prozess. Bei einem Execution Listener kann man diesen Ausführungszeitpunkt abhängig machen von unterschiedlichen Ereignissen (Events) im Prozess. Ein Task Listener dagegen reagiert nur auf Events, die mit einer Task zusammenhängen, also beispielsweise Erstellen, Zuweisen oder Beenden einer Task. Bei Task 2 wurde ein Execution Listener definiert, der eine Ankündigungsmail an alle User versendet, die das neue Soft-

warepaket erhalten. Die Mail wird versendet, wenn der Bearbeiter die Task beendet. Auf diesen Zeitpunkt hätte man auch mit einem Task Listener reagieren können. Zu Demonstrationszwecken wurde in diesem Beispiel jedoch ein Execution Listener verwendet, der gemäß Abbildung 28 unter Properties in der Kategorie Listener definiert wurde.

User Task "2 Ankündigungs-mail versenden"

General | Multi Instance | **Listener** | Form Fields

Executio...steners:

Class	Delegate Expression	Expression	Event
mail.Ankuendigungsmail			end

Add or remove table entry by right-click.

Abb. 28: Definition eines Execution Listeners

Im Beispiel wird die Javaklasse Ankuendigungsmail aus dem Package mail aufgerufen. In dieser Klasse wird per Java Mail eine Ankündigungsmail versendet. Abbildung 29 zeigt, wie ein Execution Listener in der Klasse Ankuendigungsmail implementiert wird.

```
public class Ankuendigungsmail implements ExecutionListener {

    public void notify(DelegateExecution execution) throws Exception {
        String swpaket = (String) execution.getVariable("swpaket");
        String datum = (String) execution.getVariable("datum");
        String adresse = "peter_meter5@gmx.de";
        sendMail(adresse, swpaket, datum);
    }
```

Abb. 29: Implementierung eines Execution Listeners

Beim Aufruf der Klasse Ankuendigungsmail wird die Methode notify() aufgerufen. Der Zugriff auf Eigenschaften des Prozesses erfolgt dabei über das DelegateExecution-Objekt execution. So können Prozessvariablen abgefragt werden, die zuvor über ein HTML-Formular bei der Bearbeitung der Task abgefragt wurden, im Beispiel der Name des zu verteilenden Softwarepaketes und das Datum der Verteilung.

```
<form class="form-horizontal">
<div class="control-group">
<label class="control-label">Datum der Verteilung </label>
<div class="controls">
<input form-field type="string" name="datum" />
</div>
</div>
<div class="control-group">
<label class="control-label">Name des Softwarepakets </label>
<div class="controls">
<input form-field type="string" name="swpaket" />
</div>
</div>
</form>
```

Abb. 30: HTML-Formular zu Task 2

Abbildung 30 zeigt das zugehörige HTML-Formular, das im Feld **Form Key** mit der Task verknüpft wurde. Im Beispiel wird die Ankündigungsmail exemplarisch nur an eine Person versendet. In der Realität enthält der String adresse kommasepariert alle Mailadressen der Anwender, die ein neues Softwarepaket erhalten. Dieser String kann zum Beispiel zuvor durch eine LDAP-Abfrage gefüllt werden.

In einem Prozess, in dem Aufgaben zu unterschiedlichen Zeiten von verschiedenen Bearbeitern ausgeführt werden, ist es sinnvoll, den Bearbeiter zu Beginn einer Task zu informieren, dass er nun an der Reihe ist. Diese Information kann zum Beispiel per Mail versendet werden. Dazu wird die Methode notify() gemäß Abbildung 31 verändert.

```
public class Startmail implements ExecutionListener {
    String task = null;
    public void notify(DelegateExecution execution) throws Exception {
        task=execution.getCurrentActivityName();
        String adresse = (String) execution.getVariable("adr"+execution.getCurrentActivityId());
        sendMail(adresse);
    }
```

Abb. 31: Implementierung zum Versenden einer Startmail

Die Mail wird nur an den Bearbeiter der Aufgabe versendet. Dessen Mailadresse befindet sich in der vorher erzeugten Prozessvariable mit dem Aufbau adrAKTUELLETASKID

In der Variable task wird der Name der aktuellen Task gespeichert. Daher kann in der Methode sendMail() der Betreff und Inhalt der Mail dynamisch erzeugt werden.

```
message.setSubject("Ausführen der Task " + task);
String htmlText = "Bitte führen Sie die Task <b>"
        + task
        + "</b> jetzt aus und bestätigen Sie die Durchführung in Camunda Tasklist.";
message.setContent(htmlText, "text/html; charset=utf-8");
```

Abb. 32: Verwendung von Prozessvariablen in einer Java-Methode

4.2.4 Ablaufsteuerung durch exklusive Gateways

Manchmal stellt man in einem Prozessschritt fest, dass bereits ausgeführte Aufgaben wiederholt werden müssen (Retry), beispielsweise weil ihre Bearbeitung fehlerhaft war. Exklusive Gateways ermöglichen die Abbildung von Ablauflogik im Prozess.

Abb. 33: Prozess mit exklusivem Gateway

Der Prozess in Abbildung 33 erfragt über ein Formular bei Task 4, ob das Testen der Software erfolgreich und ohne Fehler verlaufen ist. Falls ja, wird der Prozess beendet. Falls nein, wird das Softwarepaket nachgebessert und erneut bereitgestellt (Retry von Task 3) und es erfolgt ein weiterer Test (Retry Task 4). Die Bedingungen werden dabei an den vom Gateway ausgehend Sequence Flows definiert (siehe Abbildung 34).

```
<bpmn2:sequenceFlow id="SequenceFlow_14" name="Test erfolgreich"
    sourceRef="ExclusiveGateway_3" targetRef="EndEvent_5">
        <bpmn2:conditionExpression xsi:type="bpmn2:tFormalExpression">
        ${testergebnis == 1}</bpmn2:conditionExpression>
</bpmn2:sequenceFlow>
```

Abb. 34: XML-Repräsentation einer Ablaufbedingung

Falls die Variable testergebnis bei der Auswertung zur Laufzeit den Wert 1 aufweist, wird SequenceFlow14 ausgeführt. Die Variable testergebnis kann dabei zum Beispiel über ein Formular gesetzt worden sein. Es ist möglich einen Default Sequence Flow auszuwählen, falls sich keine der Bedingungen zur Laufzeit als wahr herausstellt. Wird kein Default Sequence Flow definiert und keine Bedingung ist erfüllt, tritt ein Fehler auf und der Prozess

bleibt solange an der Stelle des Gateways, bis eine der Bedingungen erfüllt ist. Es erfolgt also kein Abbruch des Prozesses. Bei der Angabe der Bedingung (condition) ist es auch möglich, eine Methode in einer Java-Klasse aufzurufen, die das Ergebnis der Auswertung als Boolean zurückgibt. Diese Funktionalität ermöglicht die Auswertung von komplexen Bed-ingungen.

4.2.5 Kapselung von Funktionalitäten durch Call Activity

Besonders bei sehr komplexen und umfangreichen Prozessen bietet es sich an, zusammen-gehörige Tasks zu Funktionalitäten zusammenzufassen und jeweils in eigene Diagramme auch in andere Projekte auszulagern. Dieser Vorgang wird als Kapselung bezeichnet. Von einem Gesamtprozess aus können diese Funktionalitäten, die nun in Subprozessen verwal-tet werden, über Call Activities aufgerufen werden. Bei den Properties der Task im Gesamt-prozess in der Kategorie General muss dann bei **Called Element** die Process **Id** des aufge-rufenen Prozesses angegeben werden. Bei Element Binding wird die Version des aufgerufe-nen Prozesses festgelegt, die verwendet werden soll. Im in der Abbildung 35 erkennbaren Beispiel ist das die aktuellste zur Verfügung stehende Version (latest).

Abb. 35: Properties der Call Activity Task 5

Sobald der Prozess an der Stelle der Call Activity angekommen ist, wird der Gesamtprozess verlassen und der Subprozess ausgeführt. Dabei können durch Setzen des Hakens bei **All Variables** (bei **Properties** in der Kategorie **General** zu finden) alle Prozessvariablen des Gesamtprozesses an den Subprozess übergeben werden (siehe Abbildung 36).

All Variables: ☑ Pass all process variables from mainprocess to the subprocess. See for more information user guide.

Abb. 36: Übergabe der Prozessvariablen an den Subprozess

Wenn der Subprozess beendet ist, wird der Gesamtprozess an der Stelle hinter der Call Activity fortgesetzt. Abbildung 37 zeigt, wie die Prozessvariablen des Subprozesses an den Gesamtprozess übergeben werden können. Dies ist beispielsweise sinnvoll, wenn die Prozessvariablen des Gesamtprozesses im Subprozess verändert wurden.

All Variables: ☑ Pass all process variables from subprocess to mainprocess. See for more information user guide.

Abb. 37: Übergabe der Prozessvariablen an den Gesamtprozess

4.2.6 Zeitgesteuerte Ausführung von Tasks durch Timer und Alarm

In einigen Fällen dürfen Tasks erst ab einer bestimmten Uhrzeit durchgeführt werden. Ein Beispiel hierfür ist die Bearbeitung von Tasks außerhalb der Kernarbeitszeit von Mitarbeitern. Für diese Aufgaben ist eine Zeitsteuerung notwendig. Abbildung 38 zeigt einen Prozess mit Zeitsteuerungselementen.

Start
5.1 Ermittlung nicht erreichter Clients
5.2 Verteilung des Softwarepakets
5.3 Installation des Softwarepakets
Ende
5.4 Alarm-Mail an Admin
Ende

Abb. 38: Prozess mit Zeitsteuerung

Der in Abbildung 38 rot markierte Abschnitt zeigt einen Timer, der den Prozesslablauf unterbricht, bis eine bestimmte Uhrzeit erreicht ist. Dazu wird ein Intermediate Catch Event mit einer Timer Definition verwendet. Die dabei angegebene Uhrzeit muss im Format ISO 8601 definiert werden, also zum Beispiel 2014-01-17T11:42:00 für den 17. Januar 2014 11:42:00 Uhr. Abbildung 39 zeigt, wie ein solcher Timer im XML definiert wird.

```
<bpmn2:intermediateCatchEvent id="IntermediateCatchEvent_1">
      <bpmn2:incoming>SequenceFlow_2</bpmn2:incoming>
      <bpmn2:outgoing>SequenceFlow_3</bpmn2:outgoing>
      <bpmn2:timerEventDefinition id="_TimerEventDefinition_2">
        <bpmn2:timeDate xsi:type="bpmn2:tFormalExpression">2014-01-17T11:42:00</bpmn2:timeDate>
      </bpmn2:timerEventDefinition>
 </bpmn2:intermediateCatchEvent>
```

Abb. 39: XML-Repräsentation eines Timers

Das in Abbildung 38 grün markierte Symbol zeigt ein Timer Boundary Event, welches verwendet wird, um eine Alarmfunktionalität umzusetzen. Wenn die Bearbeitung der Task 5.3 länger dauert, als 30 Minuten, wird der Sequence Flow ausgeführt, der das Boundary Event verlässt. Im Beispiel wird eine Alarmmail an den Koordinator versendet.

Abb. 40: Definition eines Alarms

Abbildung 40 erläutert, wie ein Alarm im Modeler bei den **Properties** in der Kategorie **Event** definiert wird. Im Feld **Duration** wird die geplante Dauer der Ausführung einer Task angegeben. Nach Ablauf dieser Dauer wird der alternative Ablauf durchgeführt. Mit einem Haken bei Cancel Activity kann festgelegt werden, dass die Task nach Auslösen des Alarms abgebrochen wird und nur noch der alternative Ablauf unter dem Boundary Event durchgeführt wird. Im Beispiel ist der Haken nicht gesetzt. Das heißt, dass die Task 5.4 ausgeführt wird und trotzdem die Task 5.3 regulär beendet werden kann. Dies erkennt man im Diagramm in Abbildung 38 an den unterbrochenen Umrandungen des Timer Events. Diese Funktionalität kann für Tasks genutzt werden, deren Ausführung auch bei Zeitüberschreitung elementar für den weiteren Prozessablauf ist und die daher nicht abgebrochen werden dürfen. Durch die Alarmmail hat der Administrator die Möglichkeit den weiteren Ablauf zu beeinflussen und möglicherweise Ablaufalternativen anzustoßen.

Bei der Task 5.4 handelt es sich um eine Service Task, das heißt, es wird kein Bearbeiter zur Durchführung der Aufgabe benötigt. Die Aufgabe wird automatisch durch Aufruf einer Java-Klasse ausgeführt. Im Bereich der Service Tasks besteht großes Potenzial zur Prozessautomatisierung, da prinzipiell alle Möglichkeiten von Java genutzt werden können.

4.3 Weiterführende Konzepte für die Prozessunterstützung durch das Workflow-Management-System camunda

4.3.1 Kontinuierlicher Verbesserungsprozess durch Aufbereitung einer Log-Datei

Da ein Workflow normalerweise wiederholt verwendet wird, ist es wichtig, diesen kontinuierlich zu verbessen. Hierbei bietet es sich an, Informationen der Ausführungen vergangener Prozesse aufzubereiten und daraus Verbesserungspotenziale abzuleiten. Camunda bietet für den Abruf von Informationen zu beendeten Prozessinstanzen einen History Service an. Dieser bietet jedoch nicht Zugriff auf alle für die Prozessverbesserung relevanten Daten. Beispielweise ist es sinnvoll, in der Log-Datei auch den tatsächlichen Bearbeiter einer Task zu speichern, da sich dieser während der Prozessausführung ändern kann. Falls Rückfragen zu einer bestimmten Task entstehen, ist der Ansprechpartner auf diese Weise direkt erkennbar. Diese individuelle Log-Datei kann mit Daten erzeugt werden, die durch Task Listener jeweils zu Beginn und Ende einer Task als Prozessvariablen zwischengespeichert werden. Nach Beendigung der Prozessinstanz werden die Logginginformationen als aufbereiteter Bericht per Mail versendet.

4.3.2 Initialisierung von Prozessvariablen über eine Konfigurationsdatei

Nicht immer sind bereits bei der Modellierung des Workflows alle Parameter, wie beispielsweise die Startzeit eines Prozesses, bekannt. Daher besteht die Anforderung, zur Laufzeit Prozessvariablen aus einer Konfigurationsdatei auszulesen. Als Dateiformat für die Konfigurationsdatei bietet sich XML an. Die Konfigurationsdatei wird zur Laufzeit von einer Java-Klasse ausgelesen und zu den Attributwerten werden Prozessvariablen erstellt, die von der Workflow-Engine verwendet werden können.

Beispielsweise ist es sinnvoll, den Bearbeiter einer Aufgabe nicht beim Modellieren statisch zu setzen. sondern das Setzen durch das Füllen einer Variablen zur Laufzeit dynamisch zu gestalten. Durch diese Funktion entfällt die erneute Modellierung eines mehrmals verwendeten Workflows, wenn sich der Bearbeiter einer Aufgabe ändert.

Assignee: ${ausfuehrender2}

Abb. 41: Dynamisches Setzen des Bearbeiters

Abbildung 41 zeigt, wie der Bearbeiter von Task 2 dynamisch gesetzt wird. Statt die Benutzerkennung des Bearbeiters in das Feld **Assignee** zu übertragen, wird eine Variable nach dem Aufbau ${VARIABLENNAME} verwendet. Diese wird durch eine Konfigurationsdatei zur Laufzeit befüllt. Dazu wird der bekannte Beispielprozess um die Task „7 Prozessinitialisierung“ erweitert. In Abbildung 42 wird der ergänzte Prozess dargestellt.

Abb. 42: Der erweiterte Beispielprozess

Die Task 7 wird von admin durchgeführt, der lediglich bestätigen soll, dass die Konfigurationsdatei in einem verwendbaren Stand vorliegt. Nach der Bestätigung wird diese gelesen. Felder, wie Bearbeiter und deren Mailadressen werden mit dem Inhalt der ausgelesenen Datei befüllt. Auch die Startzeit von Task 5.2 und die Dauer von Task 5.3 werden über die Konfigurationsdatei eingelesen. Abbildung 43 zeigt den Aufbau des dazu verwendeten XMLs. Alle nicht relevanten Attribute haben den Inhalt null.

```
<Aktivitaet>
    <ID>UserTask_4</ID>
    <Name>Softwarepaket testen</Name>
    <Beschreibung>Das Softwarepaket wird getestet.</Beschreibung>
    <GeplanterStart>null</GeplanterStart>
    <SpaetesterStart>null</SpaetesterStart>
    <Laufzeit>null</Laufzeit>
    <Ausfuehrender>tester</Ausfuehrender>
    <Mail-Exec>peter_meter5@gmx.de</Mail-Exec>
    <Kommentare>null</Kommentare>
</Aktivitaet>
```

Abb. 43: Definition einer Task in der Konfigurationsdatei

Die Attribute aus der Konfigurationsdatei werden in einer Java-Klasse in eine ArrayList geschrieben und lokalen Variablen zugewiesen. Alle relevanten Variablen werden dann gemäß Abbildung 44 der Workflow-Engine zur Verfügung gestellt.

```
task.setVariable("ausfuehrender2", Ausfuehrender2);
task.setVariable("ausfuehrender3", Ausfuehrender3);
task.setVariable("ausfuehrender4", Ausfuehrender4);
task.setVariable("ausfuehrender6", Ausfuehrender6);
task.setVariable("ausfuehrender5_1", SAusfuehrender1);
task.setVariable("ausfuehrender5_2", SAusfuehrender2);
task.setVariable("ausfuehrender5_3", SAusfuehrender3);

task.setVariable("startzeit5_2", SGeplanterStart2);
task.setVariable("dauer5_3", SLaufzeit3);
```

Abb. 44: Setzen der Prozessvariablen nach den Werten der Konfigurationsdatei

Im Beispielprozess werden zudem die Mailadressen als Prozessvariablen gesetzt, damit beim Start einer Task der Bearbeiter über den Beginn seiner Aufgabe informiert werden kann.

Um den Komfort bei der Verwaltung der Attribute in der Konfigurationsdatei zu erhöhen, wurde eine Möglichkeit entwickelt, die Konfigurationsdatei in Excel zu pflegen. Das Ändern workflowrelevanter Daten kann so auch durch Mitarbeiter ohne XML-Kenntnisse durchgeführt werden. Die Inhalte der Excel-Datei werden im XML-Format exportiert, sodass sie anschließend der Workflow-Engine zur Verfügung stehen. Die Umsetzung ist mit Excel-Standardfunktionalitäten folgendermaßen möglich.

Das Excel besteht aus neun Spalten und hat den folgenden Aufbau.

	A	B	C	D	E	F	G	H	I
1	ID	Name	Beschreibung	GeplanterStart	SpaetesterStart	Laufzeit	Ausfuehrender	Mail-Exec	Kommentare
2	M1A2	Ankuendigung_Senden	Eine Ankuendingungsmail wird an die Mitarbeiter versandt.	null	null	null	null	Example	null
3	M2S3	SW-Paket_Bereitstellen	null	null	null	null	null	null	null
4	M3S4	SW-Paket_Testen	null	null	null	null	null	null	null
5	M4B6	Bericht_Versenden	null	null	null	null	null	null	null
6	S1E51	Ermittlung_Clients_Offline	null	null	null	null	null	null	null
7	S2V52	Verteilung_SW-Paket	null	null	null	null	null	null	null
8	S3I53	Installation_SW-Paket	null	null	null	null	null	null	null
9	S4A54	Alarm_Email_Admin	null	null	null	null	null	null	null

Abb. 45: Das Excel für die Datenerfassung

Um Fehler beim späteren Umsetzen in das XML-Format bzw. später beim Einlesen in Java-Variablen zu vermeiden, sind nicht benutzte Felder unbedingt mit einem null zu füllen. Um aus diesem Excel-Blatt ein XML zu erstellen, muss ein Makro erstellt werden, dass dem Excel mitteilt, welche Spalte später welchem Tag im XML-Dokument zugewiesen werden soll.

Um dieses Makro zu erstellen, drückt man gleichzeitig die Tasten Alt und F11, um in den VBA-Modus von Excel zu wechseln. Nach den Klicks auf Einfügen und Modul erscheint ein neues leeres Modul. In dieses muss der folgende Code eingetragen werden.

```
Sub Create_XSD()
    Dim StrMyXml As String, MyMap As XmlMap
    Dim StrMySchema As String
    StrMyXml = "<AktivitaetsParameter>"
    StrMyXml = StrMyXml & "<Aktivitaet>"

    StrMyXml = StrMyXml & "<ID>Text</ID>"
    StrMyXml = StrMyXml & "<Name>Text</Name>"
    StrMyXml = StrMyXml & "<Beschreibung>Text</Beschreibung>"
    StrMyXml = StrMyXml & "<GeplanterStart>Text</GeplanterStart>"
    StrMyXml = StrMyXml & "<SpaetesterStart>Text</SpaetesterStart>"
    StrMyXml = StrMyXml & "<Laufzeit>Text</Laufzeit>"
    StrMyXml = StrMyXml & "<Ausfuehrender>Text</Ausfuehrender>"
    StrMyXml = StrMyXml & "<Mail-Exec>Text</Mail-Exec>"
    StrMyXml = StrMyXml & "<Kommentare>Text</Kommentare>"
    StrMyXml = StrMyXml & "</Aktivitaet>"
    StrMyXml = StrMyXml & "<Aktivitaet></Aktivitaet>"
    StrMyXml = StrMyXml & "</AktivitaetsParameter>"

    ' Turn off async loading.
    Application.DisplayAlerts = False
    ' Add the string to the XmlMaps collection.
    Set MyMap = ThisWorkbook.XmlMaps.Add(StrMyXml)
    Application.DisplayAlerts = True

    ' Create an empty file and output the schema.
    StrMySchema = ThisWorkbook.XmlMaps(1).Schemas(1).XML
    Open "C:\Users\Matthias\Google Drive\Duales Studium\DHBW\5. Semester\Projekt_Team\MySchema.xsd" For Output As #1
    Print #1, StrMySchema
    Close #1
End Sub
```

Abb. 46: Der VBA-Code

Zu Beginn gibt man an, welches die Begrenzenden Elemente sind (rot markiert). Hierbei sind <AktivitaetsParameter> und </AktivitaetsParameter> die obersten Knoten und begrenzen das gesamte XML. Die Tags <Aktivitaet> und </Aktivitaet> grenzen im späteren XML jeden Datensatz voneinander ab. Der grün markierte Teil sind die Tags, denen später die jeweiligen Attribute zugewiesen werden sollen. Bei der lila markierten Pfadangabe wird ein Pfad angegeben, wo Excel die sogenannte Schemadatei ablegt. Anschließend kann der Editor geschlossen und das Makro unter dem Reiter Entwicklertools im Excelblatt ausgeführt werden. Sollte der Reiter nicht angezeigt werden, muss er über Start/Optionen/Menüband anpassen aktiviert werden. Meldet Excel während der Ausführung des XMLs einen Parserfehler, kann es sein, dass:

- zwischen den Klammern (<> sowie </>) und den Tagnamen ein Leerzeichen verwendet wurde,
- ein Doppelpunkt im Tagnamen verwendet wird oder
- keine Schreibrechte am Speicherort für das XML-Schema existieren.

Anschließend kann unter den Entwicklertools/Quelle eine Zuordnung per drag&drop im Excel-Blatt erstellt werden.

Abb. 47: Die Zuordnungsfelder

Wichtig ist hierbei, dass der oberste Punkt markiert und in das Excel gezogen wird.
Nun kann die Tabelle mit Elementen gefüllt und anschließend per Button Exportieren als XML-Datei an einem gewünschten Speicherort abgelegt werden.

4.3.3 Erhöhung der Flexibilität durch Implementierung eines Replan-Konzepts

In der Praxis treten bei der Bearbeitung einer Task teilweise unerwartete Fehler auf. Manche dieser Fehler erfordern die Umplanung eines bereits gestarteten Workflows.
Es gibt für die Lösung dieses Problems bereits wissenschaftliche Ansätze. Claudia Reuter von der Zühlke Management Consultants AG und Peter Dadam von der Universität Ulm (Institut für Datenbanken und Informationssysteme) haben ein Konzept entwickelt, das sich ,,Guarded Process Spaces“ (GPS) nennt. Es handelt sich dabei um ein Werkzeug, das sich gegenüber dem Modellierer wie ein Navigationssystem verhält. Dem Benutzer werden dabei verschiedene Routen zur Zielerreichung vorgeschlagen. Die Anwendung von GPS setzt allerdings voraus, dass das WfMS gewisse Funktionen für Replans aufweisen muss.[52] Diese werden von camunda jedoch nicht angeboten. Deshalb wurde im Rahmen der Seminararbeit ein Konzept entwickelt, das Replans zur Laufzeit ermöglicht und so die Flexibilität erhöht.
Die Möglichkeit des Replans muss dabei bereits bei der Modellierung eingeplant werden. Dazu wird nach einem exklusiven Gateway eine Call Activity modelliert, die für den Aufruf des umgeplanten Prozesses sorgt. Der umgeplante Prozess kann modelliert und deployt werden, während bereits eine Instanz des ursprünglichen Prozesses läuft. Bei der Modellierung des neuen Prozesses ist darauf zu achten, dass die Process **Id** des neuen Prozesses

[52] Vgl. Reuter, C./Dadam, P. (2012)

dem Eintrag im Feld **Called Element** beim ursprünglichen Prozess entspricht. Außerdem darf die Call Activiti erst aufgerufen werden, wenn der neu gestaltete Prozess bereits deployt ist.

Abb. 48: Prozess mit Replan

Abbildung 48 zeigt die Umsetzung des entwickelten Replan Konzeptes in der BPMN-Notation. Falls die Task 5.3 länger als 30 Minuten dauert, wird der alternative Ablauf unterhalb des Timer Boundary Events gestartet. An der durchgezogenen Umrandung des Timer Boundary Events erkennt man, dass Task 5.3 im Falle einer Laufzeitüberschreitung abgebrochen wird. In der Service Task 5.4 wird eine Alarm-Mail an den Administrator versendet. Dieser kann in Task 5.5 entscheiden, ob ein Replan durchgeführt werden soll oder nicht. Falls kein Replan ausgeführt werden soll, wird der Prozess beendet. Im Falle eines Replans wird ein neuer Prozess modelliert und deployt, dessen Process **Id** mit der Eigenschaft **Called Element** der Task 5.6 übereinstimmt. Anschließend wird die Call Activity 5.6 ausgeführt und dabei der geänderte Prozess aufgerufen. Nach dem Durchlaufen des geänderten Prozesses, kehrt der Ablauf in den ursprünglichen Prozess zurück. Daher muss zur Beendigung des Gesamtprozesses ein Ende-Event hinter Task 5.6 eingefügt werden.

5 Anbindung eines Frontends mit REST

Die von camunda bereitgestellten Tools Tasklist und Cockpit zum Monitoring einer laufenden Prozessinstanz sind in der Regel für einen Einsatz im Unternehmen nicht geeignet. Vielmehr wird ein unternehmensspezifisches Frontend entwickelt werden. Um diese Frontend mit den Daten der Process Engine zu verknüpfen, bietet camunda eine Representational State Transfer (REST) Schnittstelle an.

Die REST API ist eine Programmierschnittstelle, die den Zugriff auf alle Schnittstellen der Engine ermöglicht.

Die REST-Architektur basiert auf Ressourcen, die folgende Eigenschaften haben sollten.

Eigenschaft	Beschreibung
Adressierbarkeit	Alle Ressourcen müssen durch einen eindeutigen Unique Ressource Identifier (URI) erreicht werden können.
Zustandslosigkeit	Die Kommunikation muss zustandslos sein, d.h. es existieren keine Benutzersitzungen. Bei jeder einzelnen Anfrage werden die Informationen neu mitgeschickt.
Einheitliche Schnittstelle	Ein Zugriff auf die Ressourcen muss über die definierten Standardmethoden wie z.B. GET, POST, PUT oder DELETE möglich sein.[53]
Unterschiedliche Repräsentationen	Es muss möglich sein, verschiedene Repräsentation einer Ressource ausliefern zu können wie z.B. Hypertext Markup Language (HTML), JASON oder XML.[54]

Tab. 11: Eigenschaften von Ressourcen

Für die Umsetzung eines REST-Services wird prinzipiell das Hypertext-Transfer-Protokoll (HTTP) eingesetzt. So werden für den Zugriff auf eine Ressource die im HTTP-Standard definierten Operationen verwendet. Tabelle 12 enthält die wichtigsten REST-Operationen.

Operation	Bedeutung
GET	Lesender Zugriff auf eine Ressource
POST	Erstellung neuer Ressourcen inkl. URI
PUT	Erstellung oder Bearbeitung von Ressourcen mit bekannter URI
DELETE	Löschen einer Ressource

Tab. 12: REST-Operationen

Durch die Möglichkeit, über eine Schnittstelle die Ressourcen zu erreichen, ist es erdenklich, Drittsysteme über die REST API anzubinden, wie z.B. eine eigene Benutzeroberfläche. Dennoch muss sichergestellt werden, dass für die vernünftige Umsetzung einer solchen Anwendung auch alle Ressourcen erreicht werden und die notwendigen Operationen möglich sind.

[53] Vgl. Helmich, M. (2013)
[54] Vgl. Tilkov, S. (2009)

Denn entscheidend für den Einsatz von der REST-API ist, dass alle notwendigen Ressourcen erreicht werden. Leider bietet camunda nicht explizit die Information, welche Services die REST-API im Vergleich zur Java-API anbietet. So ist es sinnvoll, die Java-API mit der REST-API zu vergleichen. Je mehr Gemeinsamkeiten diese haben, desto realistischer ist die Umsetzung eines REST-Services. In der nächsten Abbildung sind die Interfaces der Java-API (Package: org.camunda.bpm.engine) zu sehen. Diese enthält die bereits in Kapitel 3.1.2 erläuterten acht Kernschnittstellen.

Methods

	Modifier and Type	Method and Description
	void	close()
1	AuthorizationService	getAuthorizationService()
2	FormService	getFormService()
3	HistoryService	getHistoryService()
4	IdentityService	getIdentityService()
5	ManagementService	getManagementService()
	String	getName() The name as specified in 'proce:
6	RepositoryService	getRepositoryService()
7	RuntimeService	getRuntimeService()
8	TaskService	getTaskService()

Abb. 49: Interfaces der Java–API

Die REST-API (Package: org.camunda.bpm.engine.rest) bietet dazu im Vergleich folgende Services:

	Methods	
	Modifier and Type	**Method and Description**
1	AuthorizationRestService	getAuthorizationRestService(Stri
	ExecutionRestService	getExecutionService(String engin
	GroupRestService	getGroupRestService(String engin
3	HistoryRestService	getHistoryRestService(String eng:
4	IdentityRestService	getIdentityRestService(String en
	JobDefinitionRestService	getJobDefinitionRestService(Stri
	JobRestService	getJobRestService(String engineN
	MessageRestService	getMessageRestService(String eng:
	ProcessDefinitionRestService	getProcessDefinitionService(Stri
	List<ProcessEngineDto>	getProcessEngineNames()
	ProcessInstanceRestService	getProcessInstanceService(String
8	TaskRestService	getTaskRestService(String enginel
	UserRestService	getUserRestService(String enginel
	VariableInstanceRestService	getVariableInstanceService(Strin

Abb. 50: Interfaces der REST-API

Der Vergleich zeigt, dass die REST-API nur vier von acht Services zur Verfügung stellt. Dennoch sind viele andere Services vorhanden, die eine genauere Analyse voraussetzen, um eine endgültige Aussage über die zur Verfügung stehenden Funktionen treffen zu können. Die restlichen Services der REST-API, die nicht in der Java-API vorhanden sind, müssen die Funktionen der im Vergleich zur Java-API fehlenden Services (Nummer 2,5,6,7) enthalten. Die Homepage von camunda bietet eine ausführliche Dokumentation über alle Methoden der REST-API. Eine genauere Suche in der REST-API Dokumentation nach den Methoden der Java-API, die bei dem obigen Vergleich bei der REST-API fehlen, sind dennoch in der REST-API vorhanden, jedoch einem Service mit anderer Bezeichnung untergeordnet. So sind zum Beispiel Methoden des Form Services in der REST-API verteilt in den Services Process Definition und Task Service. So ist es sinnvoll, die für ein REST-Service benötigten Ressourcen und Operationen zu definieren, um anschließend die Existenz dieser in der REST-API zu überprüfen. Laut camunda sind jedoch alle relevanten Ressourcen mit der REST-API zugänglich.[55]

[55] Vgl. Camunda Docs (2013)

6 Ausblick: Einführung im Unternehmen

Mit dem Workflow-Management-System camunda kann die Ablaufsteuerung von Prozessen im Unternehmen optimiert und automatisiert werden. Dabei unterstützt camunda alle Phasen des Workflow-Managements.

In der Phase der **Modellierung** stellt camunda einen Modeler als Eclipse Plug-In zur Verfügung. Dieser ermöglicht sowohl die grafische Modellierung von Workflows in der Sprache BPMN 2.0, als auch die Bearbeitung der dabei automatisch erstellten technischen Übersetzung im XML-Format. Bei einem Einsatz des Modelers im Unternehmen ist es ratsam, den Workflow übersichtlich zu halten. Dies kann durch die Kapselung von Funktionalitäten mittels call activitys erreicht werden. Außerdem sollte bereits beim Modellieren des Workflows bedacht werden, an welchen Stellen schwerwiegende Fehler auftreten können, die eine Umplanung (Replan) erfordern. Mit geringem Aufwand kann für die Umplanung zur Laufzeit das Konzept aus Kapitel 4.3.3 verwendet werden. Für Workflows mit sich ändernden Prozessparametern bietet sich außerdem die Verwendung einer Konfigurationsdatei an.

Für die **Ausführung** des modellierten Workflows ist die camunda Workflow-Engine verantwortlich. In der vorliegenden Arbeit wurden vor allem die Organisation und die Ablaufsteuerung eines Workflows automatisiert. Beispielsweise sorgt die Workflow-Engine für das automatische Starten der Tasks in der modellierten Reihenfolge. Durch den Aufruf einer Java-Klasse kann zum Start einer Task auch eine Mail an der Bearbeiter der Aufgabe versendet werden. Neben dieser Automatisierung der Organisation kann bei einem betrieblichen Einsatz auch die Durchführung der Tasks automatisiert werden, sodass auch bei der Bearbeitung der Tasdk weniger manueller Aufwand notwendig ist. Die Workflow-Engine von camunda erlaubt hierzu den Aufruf von Java-Klassen, sodass generell ein großes Spektrum von Automatisierungsmöglichkeiten gegeben ist.

Für das **Monitoring** eines Workflows zur Laufzeit stellt camunda die Tools Cockpit und Tasklist zur Verfügung. Für den Praxiseinsatz im Unternehmen bieten diese Tools einen zu geringen Detailierungsgrad. Daher erscheint es sinnvoll, ein unternehmensspezifisches Frontend zu entwerfen, das aus mehreren Tools besteht. Hierbei sollte auch unterschieden werden, von welchen Personen die einzelnen Bestandteile genutzt werden. Beispielsweise hat ein Rollout-Verantwortlicher andere Anforderungen an das Tool, als eine Führungskraft, die sich nur über den aktuellen Status des Workflows informieren will. Um diesem Frontend die Daten der Workflow-Engine zur Verfügung zu stellen, kann die Rest-Schnittstelle von camunda verwendet werden.

Neben dem Monitoring zur Laufzeit sollte besonders bei wiederholt verwendeten Workflows eine Auswertung der Ablaufdaten nach Beendigung einer Instanz stattfinden. Für diese kontinuierliche Verbesserung des Workflows sollte eine Logging-Funktion implementiert werden, die prozessspezifische Daten der Prozessausführung speichert und aufbereitet.

Die vorliegende Arbeit legt dar, wie das Workflow-Management-System camunda die Modellierung, Ausführung und das Monitoring von Workflows unterstützt. Auf der operativen Ebene können optimierte Geschäftsprozesse als Workflows automatisiert werden. Durch die Automatisierung der Organisation und der Tasks kann der manuelle Bearbeitungsaufwand deutlich reduziert werden. Zudem steigt die Transparenz bei der Ausführung von Prozessen. Durch die Aufbereitung des aktuellen Status des Prozesses ist jederzeit für einen großen Interessentenkreis nachvollziehbar, welche Aufgaben bereits beendet wurden und welche noch durchgeführt werden müssen.

Aus diesen Gründen ist die Einführung eines Workflow-Management-Systems im Unternehmen ratsam. Bei der Etablierung kann die vorliegende Dokumentation als Leitfaden genutzt werden, da die dargelegten Konzepte auf alle Workflows mit ähnlichen Anforderungen übertragen werden können. Neben der Verwendung der Basiskonzepte kann das Workflow-Management-System durch eigenständig entwickelte Konzepte an die spezifischen Anforderungen im Unternehmen angepasst werden. Auf diese Weise können Geschäftsprozesse effizient mithilfe von Workflow-Management-Systemen automatisiert werden.

Quellenverzeichnisse

Literaturverzeichnis

Bretschi, J. (1979) Intelligente Messsysteme zur Automatisierung technischer Prozesse. Grundlagen, Möglichkeiten, Grenzen, München/Wien: Oldenbourg

Eckstein, R./Casabianca M. (2002): XML. Kurz & gut, 2. Aufl., Köln: O´Reilly

Feldmayer, J./Seidenschwarz, W. (2005): Marktorientiertes Prozessmanagement, Wie Process mass customization Kundenorientierung und Prozessstandardisierung integriert, München: Vahlen

Freund, J./Götzer, K. (2008): Vom Geschäftsprozess zum Workflow, Ein Leitfaden für die Praxis, 3.Aufl., München: Hanser

Freund, J./Rücker, B. (2012): Praxishandbuch BPMN 2.0, 3. Aufl., München / Wien: Carl Hanser Verlag

Füermann, T./Dammasch, C. (2008) Prozessmanagement. Anleitung zur ständigen Prozessverbesserung, 3. Aufl., München: Hanser

Gadatsch A. (2010): Grundkurs Geschäftsprozess-Management, Methoden und Werkzeuge für die IT-Praxis ; eine Einführung für Studenten und Praktiker. 6. Aufl., Wiesbaden: Vieweg+Teubner

Gadatsch, A. (2001): Management von Geschäftsprozessen, Methoden und Werkzeuge für die IT-Praxis ; eine Einführung für Studenten und Praktiker, Braunschweig: Vieweg

Gierhake, O. (2000): Integriertes Geschäftsprozessmanagement, Effektive Organisationsgestaltung mit Workflow-, Workgroup- und Dokumentenmanagement-Systemen. 3.Aufl., Braunschweig: Vieweg

Hammer, M. (2010): What is Business Process Management?, in: Handbook on Business Process Management – Introduction, Methods, and Information Systems,

(Vom Broke, J./Rosemann, M.), Heidelberg: Springer-Verlag

Jablonski, S. (1997): Workflow-Management, Entwicklung von Anwendungen und Systemen ; Facetten einer neuen Technologie, 1. Aufl., Heidelberg: Dpunkt-Verl.

Mühlen, M. zur/Hansmann, H.(2008): Prozessmanagement – Ein Leitfaden zur prozessorientierten Organisationsgestaltung, (Hrsg.: Becker, J./Kugeler, M./Rosemann, M.), 6. Aufl., Heidelberg: Springer-Verlag

Müller, J. (2011): Strukturbasierte Verifikation von BPMN-Modellen, Wiesbaden: Vieweg+Teubner Verlag / Springer Fachmedien Wiesbaden GmbH

Österle, H. (1995): Entwurfstechniken, 2. Aufl., Berlin: Springer

Rademakers, T. (2012): Activiti in Action, Executable Business Processes in BPMN 2.0, New York: Manning

Rempp, G. u.a. (2011): Model Driven SOA, Anwendungsorientierte Methodik und Vorgehen in der Praxis, Berlin / Heidelberg: Springer-Verlag

Richter-von Hagen, C./Stucky, W. (2004): Business-Process- und Workflow-Management, Prozessverbesserung durch Prozess-Management, Stuttgart: B.G. Teubner

Schmelzer, H. J./Sesselmann, W. (2003): Geschäftsprozessmanagement in der Praxis. Kunden zufrieden stellen - Produktivität steigern - Wert erhöhen, 3. Aufl., München: Hanser

Vom Brocke, J./Rosemann, M. (2009): Handbook on business process management, Introduction, methods and information systems, London: Springer

Vossen, G./Becker, J. (1996): Geschäftsprozessmodellierung und Workflow-Management, Modelle, Methoden, Werkzeuge, Bonn: Internat. Thomson Publ

Verzeichnis der Internet- und Intranet-Quellen

BPM Akademie (o.J.)	Rollen im Prozessmanagement, http://www.bpm-akademie.de/akademie/opencms/de/wir_ueber_uns/rollen_im_prozessmanagement/, Abruf: 15.01.2014
Camunda Cycle (2013):	„BPMN 2.0 – Roundtrip with camunda Cycle“, http://www.camunda.org/bpmn/cycle-tutorial.html, Abruf 18.01.2014
Camunda Docs (2013):	“Process Engine API”, http://docs.camunda.org/latest/guides/user-guide/, Abruf: 21.01.2014
Camunda Enterprise (o. J.):	„camunda BPM Enterprise Edition“, http://www.camunda.com/bpm/enterprise/, Abruf: 18.01.2014
Camunda Features (o. J.):	„camunda BPM platform“, http://www.camunda.com/bpm/features/#Cockpit, Abruf: 18.01.2014
Camunda Reference (2013):	„BPMN 2.0 Implementation Reference“, http://docs.camunda.org/latest/api-references/bpmn20/, Abruf: 18.01.2014
Gerzmann, S./Kostka, M./ Helmich, M. (2013):	“CAP (Computer Aided Planning) mit BPMN-Editoren – Restful Webservices (1): Was ist das haupt?, https://blog.mittwald.de/webentwicklung/restful-webservices-1-was-ist-das-uberhaupt/, Abruf: 15.01.2014
Hetze, S. (2002):	Mit LDAP Accounts für Unix und Windows zentral verwalten, http://www.linux-magazin.de/Ausgaben/2002/04/Zentrale-Meldestelle, Abruf: 22.01.2014
Konsequent (o.J.)	Prozesse gestalten, Kurzbeschreibung Prozessmanagement, http://www.konsequent-sein.de/index.php/was-ist-prozessmanagement.html, Abruf: 15.01.2014

	medoc.ustuttgart_fi/FACH-0168/FACH-0168.pdf, Abruf: 19.01.2014
Meyer, M. (2013):	ein Vergleich", ftp://ftp.informatik.uni-stuttgart.de/pub/
Reuter, C./Dadam, P. (2012):	„Navigieren statt modellieren", http://dbis.eprints.uni-ulm.de/878/1/ReDa12.pdf, Abruf: 22.01.2014
Tilkov, S. (2009):	REST – Der bessere vice?, http://jaxenter.de/artikel/REST-bessere-Web-Service-167838, Abruf: 22.01.2014
WfMC (o.J.):	Workflow Management Coalition, http://www.wfmc.org/, Abruf: 27.12.2013

DHBW
Duale Hochschule
Baden-Württemberg
Stuttgart

Open Source Content-Management-Systeme

Analyse und Bewertung

Schriftliche Ausarbeitung

im Rahmen der Lehrveranstaltung „Integrationsseminar“

vorgelegt von

Daniel Weiß,

Diana Schery Acosta Mil-Homens,

Matthias Koschar

am 31.01.2014

Fakultät Wirtschaft

Studiengang Wirtschaftsinformatik

WWI2011V

Inhaltsverzeichnis

Abkürzungsverzeichnis

AIIM	**A**ssociation for **I**nformation and **I**mage **M**anagement
CM	**C**ontent-**M**anagement
CMS	**C**ontent**-M**anagement-**S**ysteme
DM	**D**okumenten**m**anagement
ECM	**E**nterprise-**C**ontent-**M**anagement
FAQ	**F**requently **A**sked **Q**uestions
OS	**O**pen **S**ource
OSS	**O**pen **S**ource **S**oftware
WCM	**W**eb-**C**ontent-**M**anagement

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Unternehmen verändern sich im Zuge des technologischen Wandels kontinuierlich. Vor allem die Entwicklungen der Informations- sowie der Kommunikationstechnologie besitzen hier eine große Relevanz. Im Informationszeitalter ist eine eigene Internetpräsenz von Unternehmen fast schon zum überlebensnotwendigen Standard geworden. Ohne diese ist es schwierig am Markt zu bestehen. Die Websites werden hierbei über Content-Management-Systeme (CMS) aufgebaut sowie weiterentwickelt. Hierbei haben sich Open Source (OS) Lösungen in der nahen Vergangenheit immer stärker etabliert, da der Funktionsumfang mittlerweile gleichwertig ist wie der von kommerziellen Lösungen. Ein wichtiger Bestandteil bei dem Aufbau einer Website, besonders in Bezug auf die Verwaltung der darauf abgelegten Inhalte, spielt das Enterprise-Content-Management (ECM). Dieses umfasst die Elemente Erfassen, Speichern, Verwalten und Bereitstellen von Inhalten im Rahmen des Webauftritts von Unternehmen. Dieser gesamte Umfang an Aufgaben wird hierbei durch spezielle Systeme übernommen, welche CMS genannt werden.

OS CMS spielen mittlerweile eine äußerst wichtige Rolle. 85% der 100.000 weltweit größten Websites werden mit OS CMS entwickelt. Bei der Betrachtung der Top 1.000.000 liegt der Wert sogar bei 95%. Dies verdeutlicht, dass OS CMS in der heutigen Zeit nicht mehr wegzudenken sind und eine sehr zentrale Rolle einnehmen. Zudem lässt sich ein weiterer Trend klar erkennen. Die Systeme, die mit PHP realisiert wurden, erfreuen sich großer Beliebtheit und finden fast ausschließlich Verwendung.[1]

Ziel dieser Arbeit ist zum einen, einen Marktüberblick über die vorhandenen OS CMS zu geben, sowie der Entwurf eines Kriterienkatalogs, auf dessen Basis die Wahl des passenden CMS getroffen werden kann. Dieser soll eine einheitliche Bewertungsgrundlage darstellen. Um die Systeme miteinander zu vergleichen, wird eine Nutzwertanalyse aufgebaut. Der konkrete Nutzen dieser Arbeit besteht in der einfachen Bewertbarkeit möglicher CMS anhand des Kriterienkataloges innerhalb der Nutzwertanalyse. Als Ergebnis der Nutzwertanalyse kann anhand der Präferenzen eines Unternehmens ein geeignetes CMS identifiziert werden, welches den jeweiligen Unternehmensanforderungen am besten entspricht. Hierbei liegt der Fokus der Arbeit auf OS-Produkten. Kommerzielle CMS werden im Rahmen der Projektarbeit nicht eingegangen.

In Kapitel 2 werden zunächst wichtige Grundlagen von OS CMS erklärt und beschrieben, was im Rahmen dieser Projektarbeit unter dem Begriff verstanden wird. Die beschriebenen Grundlagen und Begrifflichkeiten werden dem einfacheren Verständnis der weiterführenden Kapitel dienen. Im dritten Kapitel wird erörtert, welche hauptsächlichen Anforderungen große Unternehmen an ein CMS haben. Kapitel 4 gibt einen Überblick über den erstellten Katalog

[1] Vgl. Ksi Consulting (2012)

an Kriterien. Die Ausformulierung der Kriterien dient zum Verständnis, was konkret unter den einzelnen Kriterien zu verstehen ist. Anschließend folgt in Kapitel 5 eine Beschreibung, wie die Nutzwertanalyse aufgebaut ist In diesem Zusammenhang wird die Gewichtung der einzelnen Kategorien und den jeweiligen Kriterien vorgenommen. Im Anschluss daran folgt eine Erläuterung, wie sich aus einer festgelegten Gewichtung die dazugehörige Score berechnet und wie auf Grundlage dessen eine Entscheidung für ein konkretes CMS getroffen werden kann. Eine detaillierte Marktübersicht vorhandener OS CMS wird in Kapitel 6 dargestellt. Hierbei wird beschrieben, wie die exakte Vorgehensweise zur Bestimmung der zu untersuchenden Systeme war und anhand welcher Kriterien die Auswahl getroffen wurde. Im Anschluss daran folgt eine Beschreibung der einzelnen CMS und es erfolgt eine detaillierte Untersuchung von genau diesen. Abgerundet wird die Arbeit mit einer zusammenfassenden Schlussbetrachtung und einem Ausblick, was in Zukunft noch getan werden kann, um den entwickelten Kriterienkatalog optimieren zu können.

2 Grundlagen von Open Source Content-Management-Systeme

In dem folgenden Kapitel werden diverse Begrifflichkeiten rund um das Thema Content-Management (CM) näher erläutert um ein grundlegendes Verständnis zu schaffen. Hierbei erfolgt eine Abgrenzung der Begriffe ECM, CM, Web-Content-Management (WCM) und Dokumentenmanagement (DM). Zudem wird beschrieben, was unter Open Source Software (OSS) zu verstehen ist und welche Vor- und Nachteile damit verbunden sind.

2.1 Enterprise-Content-Management

Unter ECM, oder oft auch nur CM, „ist die Methodik zur Erfassung und Erschaffung, Verwaltung, Speicherung und Aufbewahrung sowie Verarbeitung von Inhalten zur Unterstützung von organisatorischen Prozessen im Unternehmen.“[2] zu verstehen. ECM gliedert sich in drei Begriffe. Unter Enterprise ist die Abgrenzung der Informationen innerhalb eines Unternehmens zu verstehen. Content steht für Informationen jeglicher Art innerhalb von elektronischen Systemen. Das Format kann hierbei völlig unterschiedlich sein. So kann die Information ein Text oder eine Bild-, Audio- oder Videodateien sein. Unter Content ist allerdings nicht nur der Inhalt von den verwalteten Texte, Audio-Dateien oder Videos gemeint, sondern auch beschreibende Metadaten wie bspw. der Autor oder der Titel. [3] Das Management beinhaltet alle Prozesse zur Speicherung, Bereitstellung, Be- und Verarbeitung sowie Verwaltung der Inhalte. Zusammengefasst lässt sich sagen, dass ECM den Umgang mit Inhalten innerhalb einer Unternehmung beschreibt. Zudem stellt es zum effizienteren, höhergültigeren und kostengünstigeren Umgang Prozesse und Werkzeuge bereit.[4] Hierbei wird vor allem das Ziel verfolgt, einen einheitlichen Zugriff auf Unternehmensinformationen zu gewährleisten und diese den Anwendern als Dienst zur Verfügung zu stellen.[5] Ein gut funktionierendes ECM kennzeichnet sich vor allem dadurch, dass der Anwender nicht merkt, damit ein ECM überhaupt vorhanden ist.[6] Ein großer Vorteil bei der Verwendung eines CMS ist zudem, dass es Redakteuren erlaubt, Inhalte dezentral zu pflegen ohne hierfür Programmierkenntnisse zu besitzen.[7]

Nachfolgende Abb. 1 gibt einen Überblick über die Funktionen und Komponenten, welche unter ECM zusammengefasst werden. Im Rahmen dieser Seminararbeit liegt der Fokus auf dem Bereich WCM. Im Kontext der Funktionalitäten eines CMS befasst sich das DM über-

[2] Fröschle, H-P./Reich, S. (2007), S. 9
[3] Vgl. Bodendorf, F. (2006), S. 100
[4] Vgl. Hinkelmann, K./Urech, R. (2010), S. 8 f.
[5] Vgl. Manhart, K./Zimmermann, M. (o. J), S. 18
[6] Vgl. Nix, M. et al. (2005), S. 104
[7] Vgl. Abts, D./Mülder, W. (2011), S. 246 f.

wiegend mit der Erfassung und Speicherung von Dokumenten sowie mit dem Zugriff auf diese. Bei dem WCM geht es hingegen überwiegend um die Archivierung von und den Zugriff auf Content. Der wichtigste Bestandteil stellt hierbei die Ausgabe von Inhalten dar. Darunter ist die Anzeige des Contents für die Anwender zu verstehen.

Abb. 1: Funktionen und Komponenten von ECM[8]

Zur Bewerkstelligung all dieser Aufgaben, wird in Unternehmen zumeist ein CMS eingesetzt. Ein CMS bietet hierbei Funktionalitäten an, die das CM technisch unterstützen. Dies sind vor allem unterstützende Funktionen von dispositiver (z.B. Organisation des Inhalts) und operativer Aufgaben (z.B. erfassen, bearbeiten und veröffentlichen von Inhalten) sowie unterstützender Tätigkeiten (z.B. Administration des Systems). Eine wesentliche Aufgabe des CMS ist die Speicherung von Inhalten, Steuerungsinformationen und Metadaten. Mit dem Einsatz eines CMS werden prinzipiell zwei Ziele verfolgt. Zum einen sollen Kosten gesenkt und zum anderen soll zugleich die Qualität der bereitgestellten Inhalte erhöht werden. Die Kostensenkung kann durch eine Steigerung der Effizienz sowie durch eine Verkürzung der Durchlaufzeit erreicht werden. Zur Qualitätssteigerung trägt vor allem die erleichterte Pflege des be-

[8] Enthalten in: Hinkelmann, K./Urech, R. (2010), S. 13

reitgestellten Content, z.B. durch automatisches Versionsmanagement, bei. Versionen definieren den Zustand von Dateien zu bestimmten Zeitpunkten. Dabei wird bei jeder Änderung eine neue Version angelegt, um ein Zurücksetzen der Dateistände auf einen früheren Stand zu ermöglichen. Um Inkonsistenzen bei der zeitgleichen Bearbeitung einer Datei zu vermeiden, ist eine Zugriffsverwaltung notwendig. Hierbei gibt es zwei Möglichkeiten. Der Schreibzugriff der Datei wird während der Bearbeitung durch einen Nutzer für andere Nutzer gesperrt oder die zu bearbeitende Datei wird lokal auf den Rechner den Nutzers geladen (ausgecheckt) und ist erst nach erneutem Hochladen der abgeänderten Version (einchecken) für andere Nutzer wieder bearbeitbar. Das CMS ist darüber hinaus in der Lage Benutzer und deren Zugriffsrechte zu verwalten. Den Benutzern werden in der Regel definierte Rollen zugewiesen, denen bestimmte Berechtigungen hinterlegt sind. Diese Rechte beziehen sich auf Operationen wie das Lesen oder Bearbeiten von Dokumenten und auf Objekte wie das Bearbeiten des Seitenlayouts oder Erstellen eines Beitrages und können diese einschränken. Hierbei werden alle Zugriffe protokolliert, um Bearbeitungen nachvollziehen zu können.[9]

Der Content, der über das CMS verwaltet werden soll, muss zumeist aus verschiedenen Quellen wie Datenbanken, ERP-Systemen, Archiven, E-Mail oder Papierdokumente zusammengeführt werden.[10] Die folgenden drei Anforderungen werden an ein CMS gestellt:

- Integrative Middleware
  - Es sollen die möglichen Restriktionen der bisherigen Anwendungen und Insellösungen überwunden werden.
  - Der Anwender merkt nicht, dass er ein CMS verwendet.
- Funktionalitäten zur Informationsverwaltung als unabhängige Dienste
  - Die Funktionalitäten werden als Dienst bereitgestellt, welcher von verschiedensten Anwendungen genutzt werden kann.
- Verwaltung aller Informationstypen
  - Ablage der Unternehmensinformationen in einem einheitlich strukturierten Repository, welcher wiederrum alle benötigten Informationen bereitstellt.
  - Redundanzen und die Gefahr von Inkonsistenz der Informationen werden verringert.[11]

Kategorisierung der ECM Komponenten nach dem AIIM (Association for Information and Image Management):

- Erfassung (Capture): Hierbei geht es vor allem um das Input-Management. Dieses beinhaltet Aufgaben wie das Digitalisieren von Papierdokumenten oder die Einbindung von E-Mails und anderer elektronischer Dokumente. Es umfasst Funktionalitä-

[9] Vgl. Bodendorf, F. (2006), S. 100 ff.
[10] Vgl. Manhart, K./Zimmermann, M. (o. J), S. 18
[11] Vgl. ebenda, S. 104 f.

ten wie die Erfassung von Informationen bis zur Indexierung und Generierung von Metadaten mittels Texterkennung, automatischer Klassifikation und Informationsextraktion.

- Verwaltung (Manage): Bei dieser Kategorie geht es vor allem um die Verwaltung von Inhalten und Zugriffsrechten. Dies ist vor allem elementarer Bestandteil im DM, Records-Management, Workflow-Management oder in der Kollaboration.
- Ausgabe (Deliver): Vor allem die Bereitstellung von Informationen steht hier im Fokus. Das Output-Management umfasst die Aufbereitung und das Verfügbarmachen von Inhalten, sodass diese vom Anwender verarbeitet, für das System als Eingabe verwendet oder auf Endgeräten ausgegeben werden können.
- Langfristige Sicherung (Preserve): Archivierung von Informationen zur langfristig unveränderbaren Aufbewahrung und Sicherung von Informationen. Diese Funktionalität ist von elementarer Bedeutung für die Einhaltung der gesetzlichen Aufbewahrungspflichten (Compliance).
- Speicherung (Store): Temporäres Speichern von Informationen, die (noch) nicht archivierungswürdig oder archivierungspflichtig sind. In diese Kategorie gehört auch das Sichern von Daten[12]

Die folgende Abb. 2 zeigt zusammenfassend nochmals alle fünf Kategorien.

Abb. 2: Die verschiedenen ECM-Komponenten nach AIIM[13]

[12] Vgl. Hinkelmann, K./Urech, R. (2010), S. 9
[13] Enthalten in: Riggert, W. (2009), S. 6

Gründe für den Einsatz von ECM:

- Falsche Ablage von Informationen
  - Hohe Zeitaufwand für Informationssuche
  - Zeit- und Kostenaufwand für die Wiederherstellung eines Dokuments
- Verlust von Dokumenten
- Große Ansammlung von Papierdokumenten im Unternehmen
- Große Netzwerkbelastung durch das Versenden von E-Mails mit großen Anhängen.
- Gewährleistung von berechtigten Zugriffe auf vertrauliche Informationen
- Redundanzen und Medienbrüche
- Gesetzliche Anforderung zur Aufbewahrung bestimmter Informationen[14]

Bei der Verwendung von ECM ergeben sich zwei Ausprägungen, bei denen der Schwerpunkt entweder auf dem Domentenmanagement (DM) oder dem WCM liegt. In der folgenden Tab. 1 sind die beiden Ausprägungen gegenübergestellt. Eine detaillierte Beschreibung was unter DM und WCM zu verstehen ist, folgt in den nachfolgenden Kapiteln.

ECM mit Schwerpunkt DM	ECM mit Schwerpunkt WCM
Verwaltung, Nutzung und Bearbeitung aller unternehmensrelevanten Dokumente	Informationsbereitstellung und -verwaltung im Internet und Intranet
Die eigentliche Informationsdarstellung erfolgt hierbei über spezielle Systeme, deren Aufgabenschwerpunkt das DM darstellt	Grundlegende Funktionen zur Informationsverwaltung und -bearbeitung werden in dieser Ausprägung von einem System zur Verfügung gestellt

Tab 1: Abgrenzung von ECM/DM und ECM/WCM[15]

2.2 Dokumentenmanagement

Das DM bildet, wie in Abb. 1 dargestellt, lediglich eine Komponente des ECM ab. Es dient der digitalen Ablage sowie der dauerhaften Speicherung von Dateien und Dokumenten jeglicher Art und ermöglichst einen schnellen Zugriff auf genau diese. Es geht vor allem um die Erzeugung, Erfassung, Ablage, Verwaltung sowie das Wiederauffinden und Weiterverarbei-

[14] Vgl. Hinkelmann, K./Urech, R. (2010), S. 14 f.
[15] Manhart, K./Zimmermann, M. (o. J.), S. 20

ten von Dokumenten.[16] Technisch werden diese Anforderungen durch den Einsatz eines DMS unterstützt. Hierbei werden folgende Ziele verfolgt:

- Schnelle Verfügbarkeit von Dokumenten durch eine schnelle und unkomplizierte Suche.
- Revisionssichere Speicherung jeglicher Dokumente, die einer gesetzlichen Aufbewahrungsfrist unterliegen.
- Kompakte und somit speicherplatzschonende Aufbewahrung.
- Berechtigungsabhängiger Zugriff auf Dokumente, sodass keine Papierakten mehr versendet werden müssen.[17]

2.3 Web-Content-Management

Zunächst müssen die Begrifflichkeiten CM und WCM differenziert betrachtet werden. Es ist häufig der Fall, dass die beiden Begriffe als Synonym verwendet werden. Eine solche gleichbedeutende Verwendung ist allerdings falsch. Es lassen sich die beiden Begrifflichkeiten in ihrer Bedeutung wie folgt abgrenzen. Bei WCM liegt der Fokus vor allem auf die Veröffentlichung und Verwaltung von Inhalten in Internetseiten, wohingegen unter CM die Verwaltung jeglicher Datei- und Medienformate, wie bspw. MS Office Dokumente oder Bild-, Audio-, und Videodateien[18], verstanden wird. Der Übergang zwischen den beiden Begriffen ist allerdings fließend.[19] Zusammengefasst lässt sich sagen, dass unter CM die Verwaltung von Dateien verstanden wird und unter WCM die Verwaltung von radaktionell abgelegten Texten und sonstigen Inhalten auf einer Webseite.

Die drei Säulen eines WCM sind in der folgenden Abb. 3 ersichtlich. Hierbei wird das CM um die Web-Komponente erweitert. Die drei Säulen lassen sich durch den Einsatz eines Systems optimal unterstützen.

[16] Vgl. Abts, D./Mülder, W. (2011), S. 246 f.
[17] Vgl. ebenda, S. 219
[18] Vgl. jdk (o. J.)
[19] Vgl. Larisch, D. (2011), S. 131

Web	Content	Management
- Internet - Intranet - Extranet	- Text - Grafiken - Soundfiles - Animation - Video	- Erstellung - Veränderung - Speicherung - Suche - Transport - Publikation - Archivierung
System		

Abb. 3: Aufbau von Content-Management-Systemen [20]

2.4 Open Source

Unter OS ist ein Konzept zu verstehen, „nach dem Programme mit ihrem Quellcode ausgeliefert werden. Jeder darf den Quellcode einsehen und verändern. Die Open Source Initiative definiert Kriterien, die OSS erfüllen soll.“[21] Bei OSS wird somit der Quellcode der Anwendung veröffentlicht und es wird en Anwendern gestattet, diesen weiterzugeben und zu verändern. Bei dem Open-Source-Konzept ist dies nicht nur gestattet sondern sogar erwünscht.[22] OS bringt hierbei zahlreiche Vorteile, welche nachfolgend dargestellt werden:

- Durch die freie Verfügbarkeit des Quellcodes kann bei Unklarheiten oder Problemen direkt der Quelltext der OSS zur Hilfe genommen und gelesen werden. Das hilft vor allem zur schnellen Beseitigung von Fehlern, ohne hierbei lange auf einen Patch oder ein neues Release warten zu müssen. Zudem hilft es bei der Klärung von Fragen, die sich anhand der vorliegenden Dokumentation nicht eindeutig oder nur unvollständig klären lassen. Darüber hinaus ist es möglich, die Software an die eigenen Bedürfnisse anzupassen, in dem neue Funktionalitäten hinzugefügt, verändert oder ergänzt werden.
- Bei OSS fallen keine Lizenzkosten an. Das bringt den großen Vorteil, dass die Produkte zunächst einmal ausprobiert werden können und getestet werden kann, welche Anforderungen die Produkte abdecken können. Zudem sind OSS nicht in den Investitionsplan der Kostenplanung aufzuführen.[23]

[20] Mit Änderungen entnommen aus: Abts, D./Mülder, W. (2011), S. 247
[21] Gabler Wirtschaftslexikon (o. J.)
[22] Vgl. Abts, D./Mülder, W. (2010), S. 371
[23] Vgl. Becker-Pechau, P./Roock, S./Sauer, J. (2004), S. 20 f.

- Durch die Verwendung von OSS wird die Abhängigkeit von einzelnen Softwareherstellern reduziert, da z.B. Schnittstellen zum Datenaustausch selbst programmiert werden können.[24]

Allerdings birgt die Verwendung von OSS in Unternehmen auch gewisse Risiken. Mögliche Risiken sind nachfolgend aufgeführt:

- Durch den Einsatz von zu vielen OSS besteht die Gefahr, dass unnötige oder auch doppelte Funktionen durch die Anwendungen angeboten werden.
- Die Systemarchitektur wird durch Komponenten, die nicht zusammenpassen und zudem auf unterschiedlichen Architekturen beruhen, verkompliziert.
- Bei OSS besteht die Gefahr, dass mehrere Anwendungen für dieselben Anforderungen angeschafft werden und somit die Anwendungslandschaft unübersichtlich machen. Bei kommerziellen Anwendungen besteht die Gefahr nicht, da die Lizenzkosten regulativ wirken.
- Der offene Quellcode kann eine schlechte Dokumentation des OSS zur Folge haben. Dies erfordert somit den Blick in den Quellcode um ein Verständnis für die Software zu bekommen.[25]

Das Zusammenspiel zwischen dem Distributor einer OSS, den Softwareentwicklern und den Benutzern der OSS sieht hierbei wie folgt aus:

Die Softwareentwickler sind für die kontinuierliche Weiterentwicklung der OSS verantwortlich. Der Distributor ist der Inhaber des Urheberrechts der OSS und vertreibt die Software. Hierfür nutzt er die aktuellste Version, welche die Softwareentwickler programmiert haben und räumt diesen im Gegenzug gewisse Rechte bei der Weiterentwicklung ein. Der Anwender darf die OSS kostenfrei Nutzen und hat hierbei Zugriff auf den Quellcode und darf diesen sogar modifizieren. Zwischen dem Distributor und dem Endnutzer liegt ein Nutzungsvertrag vor. Kosten für das OSS fallen lediglich für Leistungen wie Schulungen, Serviceleistungen oder Wartungen an. In der nachfolgenden Abb. 4 ist das OS-Prinzip veranschaulicht dargestellt.

[24] Vgl. Abts, D./Mülder, W. (2010), S. 371
[25] Vgl. Becker-Pechau, P./Roock, S./Sauer, J. (2004), S. 20 f.

Software-Entwickler
Nutzung
Distributor
Verpflichtung
Nutzungsrecht
Verpflichtung
(geringe) Kosten (Wartung etc.)
Nutzungsvertrag
Benutzer

Abb. 4: Quelloffene Software[26]

OSS gibt es in einer Vielzahl unterschiedlicher Bereiche, einen davon bildet der Bereich des Content Managements. Die Systeme haben sich in Bezug auf den Funktionsumfang enorm weiterentwickelt und stehen somit kommerziellen Produkten kaum in etwas nach. Speziell in dieser Entwicklung ist auch zu erklären, weshalb OS CMS selbst für Unternehmen sehr beliebt geworden sind.

[26] Mit Änderungen entnommen aus: Abts, D./Mülder, W. (2011), S. 65

3 Anforderungen von Unternehmen

„Unabhängig von der Unternehmensgröße gibt es grundlegende Minimal-Anforderungen, die ein CMS erfüllen muss."[27] Hierzu gehört eine intuitive Anwendungsoberfläche sowie eine einfache Bedienbarkeit der Anwendung. Eine Unternehmens-Website sollte von den Mitarbeitern ohne spezielles Web-Know-how gepflegt werden können. Zudem erhöht ein leicht zu bedienendes CMS die Akzeptanz bei den Mitarbeitern und verringert zugleich den Schulungsaufwand. Zusammengefasst lässt sich sagen, dass selbst technisch versierte Mitarbeiter in der Lage sein müssen als Redakteure schnell zu guten Ergebnissen zu kommen. Zudem sollte ein CMS eine hohe Integrationsfähigkeit besitzen um technisch höchst flexibel agieren zu können. Offene Schnittstellen zu den unterschiedlichsten Software-Lösungen sind hierbei äußerst wichtig, um das CMS ohne größeren Programmieraufwand an die vorhandenen Systeme anbinden zu können. Die Gefahr von Systemen ohne offene Schnittstellen ist, dass diese zu Beginn zwar alle geforderten Kriterien entsprechen allerdings spätestens bei den ersten ungeplanten Änderungen sehr aufwändig und zeitintensiv angepasst werden müssen.[28] Ferner muss das CMS zudem ein Berechtigungskonzept beinhalten, sodass für unterschiedliche Anwender differenzierte Inhalte verfügbar sind und angezeigt werden können. Eine weitere äußerst wichtige Anforderung ist die Unterstützung eines Publishing-/ Staging-Konzeptes. Dies ermöglicht die Ablage und Bearbeitung von Inhalten in unterschiedlichen Bereichen. Es kann bspw. vor Veröffentlichung einer Änderung diese zunächst in einer Test-Umgebung getestet und erst nach erfolgreichem Test veröffentlicht werden. Weitere wichtige Kriterien in Hinblick der Zukunftssicherheit eines Systems sind die Anzahl der Entwickler, das Produktalter sowie die Veröffentlichungshäufigkeit neuer Versionen. Bei der Überlegung ein CMS im Unternehmensumfeld einzusetzen, spielt bei OSS die Zukunftssicherheit eine äußerst bedeutende Rolle. Da sich quantitative Kriterien leichter vergleichen lassen als qualitative, wurde im Rahmen dieser Arbeit entschieden, dass diese die Grundlage für eine erste Eingrenzung für die Auswahl der zu untersuchenden CMS bilden.

[27] Contentmanager.de (2013a)
[28] Vgl. ebenda

4 Kriterienkatalog

Innerhalb dieses Kapitels wird ein Kriterienkatalog entwickelt, der bei der Auswahl von CMS als Grundlage für die Entscheidung dienen soll. Ausgangspunkt hierfür war ein Gespräch mit dem Auftraggeber, in dem Vorschläge zu möglichen Kriterien gemacht wurden.[29] Dabei ließen sich drei Oberkategorien für die Kriterien bilden. Strukturiert wurden diese in generelle Kriterien für ein CMS, Kriterien, die für große Unternehmen von Bedeutung sind und Kriterien, die bei der Auswahl von OS CMS zu beachten sind. Die insgesamt ausgearbeiteten 98 konkreten Kriterien wurden in 26 Unterkategorien aufgeteilt und den jeweiligen Oberkategorien zugeordnet.

4.1 CMS allgemein

In der Kategorie ‚CMS allgemein' spielen die folgenden neun Unterkategorien eine zentrale Rolle. Damit werden alle grundlegenden Eigenschaften betrachtet die ein CMS besitzen sollte:

Technische Spezifikationen

Unter der Kategorie technische Spezifikationen werden die Eigenschaften eines CMS zusammengefasst, welche die technischen Gegebenheiten angehen. Bei der Skalierbarkeit geht es um die Erweiterbarkeit des Systems im Falle die das Performancegründen erforderlich werden sollte. Unter Wechselbarkeit der Datenbank ist zu verstehen, ob ein Austausch des Backend möglich ist und mit welchem Aufwand das verbunden ist. Das Kriterium Virtualisierung soll ausdrücken ob es möglich ist das CMS unter einer virtuellen Umgebung zu verwenden. Der Clusterbetrieb drückt letztendlich aus, ob die Möglichkeit besteht das CMS innerhalb eines Clusters von mehreren Servern zu betreiben, sodass der Content innerhalb des kompletten Clusters verfügbar ist.

Erweiterbarkeit

Bei dieser Kategorie geht es um die Erweiterbarkeit eines CMS. So wird untersucht, ob sich dieses durch Plugins (bestimmte Funktionalitäten) oder Module (Einbindung von Scripts auf dem Client) erweitern lässt. Ein weiteres Kriterium ist hierbei die Integration von Anwendungen durch Portlets (Einbindung von Scripts auf dem Server).

Suchmaschinenfreundlichkeit

Hierunter ist zu verstehen, wie einfach die erstellte Website von Suchmaschinen wie Google erfasst und somit gelistet werden können. Hierunter fällt, ob die URLs aus einer kryptischen Zeichenfolge bestehen oder sprechende Bezeichnungen enthalten. Über die Erstellung einer

[29] Vgl. Hitz, M. (2013)

Sitemap möglich ist und ob sich Metadaten zu einer Website hinterlegen lassen, welche Eigenschaften der Seite enthalten.

Funktionalitäten

Die Kategorie Funktionalitäten beinhaltet diverse Funktionen und überprüft, ob diese von dem jeweiligen CMS unterstützt werden oder nicht. Es wird geprüft, ob ein Versionsmanagement vorhanden ist, um alte Versionsstände von Content jederzeit widerherstellen zu können. Die Funktion Backup und Widerherstellungsmöglichkeit bezieht sich im Gegensatz dazu auf die komplette Website. Hierunter wird die Möglichkeit verstanden, einen bestimmten Entwicklungsstand einer Website zu sichern und diesen zu einem späteren Zeitpunkt gegebenenfalls widerherstellen zu können. Ein weiterer wichtiger Punkt ist die Möglichkeit eine lokale Kopie der Website auf einem Computer zu speichern um an dieser weiterarbeiten zu können, selbst wenn keine Internetverbindung besteht. Eine elementare Funktion eines CMS stellt zudem die Suche nach Content dar. Sollte dies nicht Möglich sein, kann dies zu zeitintensivem Durchsuchen der kompletten Website führen. Unter dem Kriterium erweiterte Funktionalitäten werden Features wie das Vorhandensein eines Wikis, Kollaborationsfunktionalitäten, Taxonomie Management, Records Management, etc. verstanden. Eine weitere Funktionalität stellt der PDF-Export dar. Dieses Kriterium beinhaltet die Möglichkeit die Webseite als ein PDF-Dokument exportieren bzw. drucken zu können. Hierbei wird die Seite allerdings zunächst aufbereitet, sodass diese übersichtlicher und strukturierter auf dem Dokument dargestellt wird. Die letzte Funktionalität dieser Kategorie beschreibt die Möglichkeit, Content zu exportieren oder von anderen CMS zu importieren.

Benutzbarkeit

Die Kategorie Benutzbarkeit beinhaltet alle Kriterien, welche für eine leichtere Handhabung des CMS beitragen. Softwareergonomie beschreibt hierbei generell wie komfortabel und intuitiv sich die Anwendung bedienen lässt. Unter Robustheit ist die Fähigkeit eines Systems zu verstehen, Veränderungen ohne Anpassungen der stabilen Anfangsstruktur standzuhalten. Barrierefreiheit beschreibt inwiefern sich das System für körperlich eingeschränkte Personen bedienen lässt. Hierbei gibt es die Unterteilung in die Besucher einer Website und die Entwickler der Website. Die direkte Navigation auf Websites beschreibt die Möglichkeit, dass bestimmte Seiten nur über die Verwendung von Direktlinks erreichbar sind. Eine weitere unterstützende Funktionalität stellt die Möglichkeit dar, Tastaturshortcuts zu konfigurieren bzw. zu verwenden. Hierdurch kann z.B. auf bestimmte Bereiche schneller zugegriffen werden. Unter dem modularen Aufbau und der Gestaltung einer Website ist die Zusammensetzung/Montage der Seite unter Verwendung von zwei oder mehreren in sich funktionsfähigen Modulen zu verstehen. Das Kriterium Personalisierbarkeit der Anwenderoberfläche beschreibt letztendlich das Customizing der Oberfläche nach dem Geschmack des Anwenders.

Kompatibilität

Hierbei wird die Kompatibilität mit dem Webstandard HTML5 überprüft. Eine weitere Anforderung ist die Unterstützung des Responsive Webdesign. Darunter ist die automatische Anpassung der Website auf das jeweilige Endgerät zu verstehen, um ein bestmögliches Erscheinungsbild zu gewährleisten. Ebenso sollte das CMS browserunabhängig betrieben werden können.

Editor

In dieser Kategorie werden alle Kriterien betrachtet, denen der Editor entsprechen sollte. Der erwartungskonforme Aufbau spielt eine sehr wichtige Rolle. Inhalte per Drag & Drop zu verschieben wäre zudem wünschenswert. Websites müssen einfach editierbar sein, wobei eine Vorschau der gemachten Änderung angezeigt werden sollte. Eine Zwischenspeicherungs- und Wiederherstellungsfunktion sollte existieren. Eine Rechtschreibprüfung, sowie die Fehlererkennung im HTML-Code würden den Anwender unterstützen. Die Integration von Anwendungen, beispielsweise über JavaScript, sollte möglich sein. Ein großer Freiraum an Gestaltungsmöglichkeiten wäre zudem von Vorteil.

Medienverwaltung

Hierrunter werden alle Kriterien verstanden, die eine Verwaltung von Medien ermöglichen. Unter Medien sind alle interaktiven Inhalte zu verstehen, bei denen es sich nicht um Dokumente im eigentlichen Sinn handelt. Prinzipiell sollte es möglich sein Medien als Content einbinden zu können. Ebenso ist es erstrebenswert, dass der Download von Medien in verschiedenen Formaten und Qualitätsstufenmöglich ist. Eine im CMS integrierte Bildbearbeitung wäre zudem vorteilhaft. Würde eine Mediengalerie im System enthalten sein, vereinfacht sich dadurch die Verwaltung der Medien. Des Weiteren sollte eine Unterstützung von Kartendiensten ermöglicht werden, sodass eine einfache Referenzierung auf geographische Standorte möglich ist.

Sonstige

Innerhalb des CMS sollte eine Trennung zwischen dem eigentlichen Inhalt, dessen Darstellung und der hinterlegten Metadaten erfolgen. Beim Erscheinen neuer Versionen ist es wünschenswert, dass die Aufwärtskompatibilität sichergestellt ist. Dies bedeutet, dass alle erstellten Inhalte in die neue Version übernommen werden können. Werden Schulungen durch einen Dienstleister für ein CMS angeboten, wäre dies sehr vorteilhaft, um beispielsweise neue Mitarbeiter einzulernen oder generell das notwendige Knowhow für die Verwendung eines CMS in das Unternehmen zu bringen. Ein Block dient zur Protokollierung und Aufzeichnung von Sachverhalten. Alle Anwender haben generell die Möglichkeit den Block zu kommentieren und darüber zu diskutieren. Es sollte zudem eine Indexseite vorhanden sein, die alle im CMS existierenden Websites alphabetisch sortiert.

4.2 Unternehmenseinsatz

Für den Einsatz eines CMS im Unternehmensumfeld sollten die folgenden Kriterien erfüllt werden, die sich in elf Unterkategorien einteilen lassen:

Plattformunabhängigkeit

Das CMS sollte plattformunabhängig funktionieren. Dabei sollte es weder an eine spezielle Ablaufumgebung noch an ein konkretes Betriebssystem gebunden sein, sondern unabhängig davon arbeiten, wie dies z.B. bei Java-Applets der Fall ist.

Unterstützung mehrsprachiger Content

Zur Unterstützung von mehrsprachigem Content sollte die Austauschbarkeit sichergestellt werden. Hierbei bietet es sich an, den Content in verschiedenen Sprachen erstellten und flexibel austauschen zu können. Ebenso sollte das CMS mit unterschiedlichen Zahlen- und Datenformaten umgehen können. Beispielsweise muss sich das Format des Datums flexibel austauschen und verändern lassen.

Sicherheit

In dieser Kategorie geht es um die Sicherheit des CMS. Hierfür sollte eine sichere Datenübertragung durch Protokolle wie https oder SSL gewährleistet werden. Die Einhaltung der Datenschutzrichtlinien eines Unternehmens stellt ein weiteres äußerst elementares Kriterium dar. Auch von außen sollte ein sicherer Zugriff auf das System erfolgen können, sodass externe Partner darauf zugreifen können.

Staging

Unter Staging ist die Überführung von Inhalten in unterschiedliche Bereiche innerhalb eines Unternehmens zu verstehen. Solche Staging-Bereiche könnte z.B. eine Entwicklungs-/Test- und Produktionsumgebung darstellen. In diesem Zusammenhang wäre es zudem äußerst wichtig, wenn eine Import- / Exportfunktionalität vorhanden wäre, um hierüber über Datenformate wie CSV oder XML Inhalte austauschen zu können.

Berechtigung innerhalb des Systems

Ein äußerst wichtiges Kriterium für große Unternehmen stellt der Bereich Berechtigungskonzept innerhalb eines Systems dar. Hierbei ist es äußerst wichtig, dass verschiedene Mandanten verwaltet werden können und diese unterschiedliche Sichten auf den Inhalt des Systems haben. Unterstützend kann hierbei durch eine Authentifizierung dem Anwender bestimmte Berechtigungen zugewiesen werden. Ferner sollte die Definition von Rollen innerhalb eines Systems möglich sein, denen bestimmte Berechtigungen zugewiesen sind. Zudem sollten Berechtigungen für Benutzer und Rollen vererbt werden können. Ein Kollisionsmanagement hilft zudem bei der Vermeidung von Inkonsistenzen bei der zeitgleichen Editierung einer Seite. Zudem sollten Berechtigungen für einzelne Inhalte wie z.B. Dokumente eingerichtet werden können, sodass diese nicht für jedermann verfügbar sind.

Aufwand

Hierunter ist zu verstehen, wie hoch der manuell zu leistende Einsatz durch Mitarbeiter oder externe Dienstleister ist. Es wird zwischen dem Aufwand der für die erstmalige Installation und Konfiguration des Systems notwendig ist, den Aufwand für den Betrieb des Systems, die Aufwendungen für die Wartung und Aufwendungen die bei der Veröffentlichung neuer Versionen auftreten können, unterschieden.

Benachrichtigung

Es sollte die Möglichkeit bestehen, Mitarbeiter durch automatisch versendete Nachrichten durch das CMS über bestimmte Umstände informieren zu können. Dies sollte vor allem über gängige Formate wie E-Mail oder SMS durchführbar sein. Zudem ist eine Unterstützung von Newsfeeds von Vorteil, da hiermit unmittelbar über Neuerungen auf der Websitesinformiert werden kann.

Schnittstellen

Hierunter wird die Kompatibilität mit Fremdsystemen wie z.B. SharePoint, die Anbindung an interne Suchmaschinen sowie die Zugriffsmöglichkeit auf Inhalte durch Webservices zusammengefasst.

Templateverwaltung/-erstellung

Unter Template wird eine Vorlage verstanden. Es muss untersucht werden, ob sich Vorlagen für komplette Websites und/oder für bestimmten Content erstellen und verwalten lassen können. Dies spielt vor allem für große Unternehmen eine zentrale Rolle, wenn sie die Website an Ihr Corporate Design anpassen möchten.

Controlling

Um ein detailliertes Controlling durchzuführen sollte eine zeitgesteuerte Bereitstellung von Websites unterstützt werden. Hierbei ist es von hoher Bedeutung, dass die Integration eines Trackingtools auf die jeweilige Website möglich ist.

Radaktionelle Freigabeprozess

Hierunter wie die erforderliche Freigabe von Inhalten vor der Veröffentlichung auf der Website verstanden. Hierbei kommt das sogenannte Vier-Augen-Prinzip zum Einsatz. Ein Redakteur erstellt hierbei den Inhalt, welcher von einem Publisher zunächst freigegeben werden muss.

4.3 Open Source

Gerade im OS-Umfeld gilt es bestimmte Kriterien zu berücksichtigen, welche in den folgenden 6 Unterkategorien beschrieben werden:

Community

In dieser Kategorie spielen die Kriterien aus wie vielen Mitgliedern die Community besteht sowie die Anzahl der Forenbeiträge eine wichtige Rolle.

Dokumentation

Hierbei geht es unter anderem um die Dokumentation des Programmiercodes. Diese Dokumentation dient zum besseren Verständnis des Programmcodes, sodass andere Entwickler das Programm weiterentwickeln und Veränderungen vornehmen können. Die sogenannten Frequently Asked Questions (FAQ) zählen ebenfalls zu dieser Kategorie. Unter FAQ ist eine Sammlung von häufig gestellten Fragen sowie die dazugehörigen Antworten zu verstehen. Auf diese Weise können die restlichen Support-Wege deutlich entlastet werden. Eine weitere Dokumentation stellt das Benutzerhandbuch dar. Dieses enthält Informationen für Anwender, sodass dieser bei der Verwendung des Systems wichtige Funktionalitäten nachlesen kann. Das Entwicklerhandbuch enthält dagegen eine technische Beschreibung der Anwendung. Es dient zum Verständnis der verwendeten Funktionen, Klassen, etc. Die Dokumentationen sollten darüber hinaus in einer verständlichen Sprache formuliert sein, sodass das Dokument nachvollziehbar ist.

Verbreitungsgrad

Unter Verbreitungsgrad ist zum einen die Anzahl der Entwickler, welche das System weiterentwickeln, zu verstehen und zum anderen wie häufig das System von potenziellen Benutzern heruntergeladen wurde. Generell lässt sich sagen, dass eine größere Anzahl an Ansprechpartnern positiver zu bewerten ist.

Support

Unter Support ist die technische und fachliche Kundenbetreuung zu verstehen. Hierbei können Entwickler, Dienstleister oder Provider die direkten Ansprechpartner für den Kunden sein. Der Support erfolgt in der Regel durch die Bearbeitung der Kundenanfragen sowie die Lösungsfindung für die dargestellten Probleme. Ein Wiki kann hierfür als Selbstsupport dienen, sodass der Anwender direkt nach seinem Anliegen suchen kann. Das Wiki kann entweder direkt in das CMS integriert oder direkt über das Internet abrufbar sein. Tutorials bezeichnet eine schriftliche oder (multi-) mediale Gebrauchsanleitung, die den Anwender bei dem Gebrauch des CMS unterstützen kann.

Aktualität

In dieser Kategorie geht es um die Aktualität des CMS. Diese drückt sich zum einen durch die Geschwindigkeit der Fehlerbehebung aus und zum anderen in welchen zeitlichen Abständen eine neue Version des CMS veröffentlicht wird.

Sonstiges

Das Kriterium Zukunftssicherheit drückt die Wahrscheinlich über das Vorhandensein des CMS in der fernen Zukunft aus. Zudem spielt bei OS Produkten der kostenfreie kommerzielle Gebrauch eine wichtige Rolle. Unter Userrating ist die Bewertung eines CMS durch die Anwender zu verstehen. Ein weiteres Kriterium ist die Anzahl der Sprachen unter denen sich das CMS entwickeln und betreiben lässt. Je mehr Sprachen von einem CMS unterstützt werden, desto höher ist die Möglichkeit, dass dieses von mehreren Entwicklern verwendet wird. Weiter kann sich ein CMS positiv hervorheben, wenn dieses in mehreren Versionen erhältlich ist. Es besteht die Möglichkeit eine kostenfreie Basisversion und eine käuflich erwerbliche Version mit umfangreichen Funktionalitäten anzubieten. Unter Popularität ist der Bekanntheitsgrad eines Systems zu verstehen. Dieser kann durch die Anzahl der bestehenden Websites, die auf Basis des CMS erstellt wurden. Unter Marktanteil ist die relative Verwendung eines CMS im Vergleich zu den anderen Systemen zu verstehen.

5 Aufbau einer Nutzwertanalyse

Um anhand der erarbeiteten Kriterien die CMS miteinander vergleichen zu können, wird eine Nutzwertanalyse aufgebaut. Dafür lässt sich die Nutzwertanalyse in zwei Bereiche teilen. Wie in Abb. 5 zu sehen ist, existiert der Bereich der definierten Vorgaben (‚Bewertungsraster', linke Seite) und der Bereich für die Bewertung der jeweiligen CMS (‚CMS Bewertung', rechte Seite).

Nutzwertanalyse von Open Source Content-Management-Systeme												
Bewertungsraster				CMS Bewertung								
				Joomla!			TYPO3			Drupal		
Kategorie	Unterkategorie/Kriterium	Gewich-tung	Scores maximal	Vorgabe/ Kommentar	Bewer-tung	Scores	Vorgabe/ Kommentar	Bewer-tung	Scores	Vorgabe/ Kommentar	Bewer-tung	Scores

Abb. 5: Bereichsaufteilung innerhalb der Nutzwertanalyse

Diese Nutzwertanalyse wird über eine Excel-Tabelle realisiert, welche auf der beiliegenden CD enthalten ist. Innerhalb dieser Tabelle sind alle Kriterien (siehe Kapitel 4.1 – 4.3) im Bewertungsraster aufgeführt, die pro System bewertet werden können. Um die Nutzwertanalyse innerhalb der Excel-Tabelle durchzuführen, werden in den folgenden Kapiteln eine Festlegung zur Gewichtungsverteilung vorgenommen, die maximal zu vergebenden Scores errechnet, eine Bewertungsskala aufgestellt sowie die tatsächliche Berechnung der Scores beschrieben.

5.1 Gewichtungsverteilung festlegen

Jedes Kriterium muss eine Gewichtung erhalten, um festzulegen, wie wichtig es für den Auswahlprozess ist. Dafür wird ein Prozentwert verwendet. Dieser wird in der Spalte ‚Gewichtung' des Bewertungsrasters festgehalten. Insgesamt können maximal 100% erreicht werden. Innerhalb der einzelnen Unterkategorien werden ebenso stets 100% verteilt. Dem Anwender bzw. Entscheidungsträger ist es jeweils frei überlassen, welche Gewichtung er zugrunde legen möchte. Zum einfacheren Einstieg in den Kriterienkatalog wurde eine Einstiegsmaske entworfen, über die es möglich ist, die Gewichtung der Oberkategorien festzulegen. Die Werte werden durch Klick auf die Schaltfläche OK direkt in den Katalog übernommen. Durch Klick auf die Schaltfläche Abbrechen wird die Maske geschlossen und gelangt so direkt auf den Kriterienkatalog. Hier besteht die Möglichkeit die Gewichtung direkt in das Tabellenblatt einzutragen. Zu beachten ist hierbei, dass die eingetragenen Werte in Summe 100 % ergeben müssen. Nachfolgend ist in Abb. 6 ein Screenshot der beschriebenen Einstiegsmaske zu sehen. Hierbei ist für die drei festgelegten Oberkategorien jeweils die

Gewichtung in das jeweilige Feld einzutragen. Die Navigation durch die Masken kann hierbei komplett mit der Tastatur oder unter Zuhilfenahme der Maus geschehen.

Abb. 6: Einstiegsmaske des Kriterienkatalogs zur Gewichtung der Oberkategorien

Nach Bestätigung der Eingaben durch die Schaltfläche OK, wird eine weitere Maske aufgerufen, worüber sich die Gewichtung der Unterkategorien festlegen lässt. Hierbei findet sich jede Oberkategorie unter einem Reiter wieder. Je nach dem welcher Reiter ausgewählt wird, werden die hierbei relevanten Unterkategorien angezeigt. Hier kann ebenfalls eine benutzerdefinierte Gewichtung eingetragen werden, welche in Summe 100% ergeben muss. Die eingetragenen Werte aller Reiter werden ebenfalls nach Bestätigung durch Klick auf die Schaltfläche OK in den Kriterienkatalog übernommen. Durch die Schaltfläche Zurück wird die Einstiegsmaske erneut aufgerufen um mögliche Änderungen an der Gewichtung der Oberkategorien vornehmen zu können. Durch Abbrechen wird die Maske geschlossen. Ein Screenshot des Formulars über das sich die Gewichtung der Unterkategorien festlegen lässt, ist hierbei in Abb. 7 zu sehen.

Abb. 7: Gewichtung der Unterkategorien

Nachdem die Gewichtung der Unterkategorien festgelegt und bestätigt wurde, besteht die Möglichkeit die einzelnen Kriterien zu gewichten. Hier können pro Unterkategorie wieder 100% verteilt werden. Eine Besonderheit stellt das Kriterium ‚Barrierefreiheit' der Unterkategorie ‚Benutzbarkeit' dar. Dieses unterteilt sich in die Punkte Besucher und Entwickler für die wiederrum komplette 100% der Gewichtung verteilt werden können. Ein Screenshot der Maske, mit welcher die Gewichtung der einzelnen Kriterien vorgenommen werden kann, ist in Anhang 1 abgebildet. Zudem sind ein Auszug des Quellcodes und eine technische Erklärung in Anhang 2 vorzufinden.

Über eine in Excel hinterlegte Formel wird die Gewichtung, welche über die Masken festgelegt werden konnte, bei der Berechnung der Scores (siehe Kapitel 5.4) berücksichtigt. Diese Formel bringt über das Element der ‚maximalen Scores' den Vorteil, dass veränderte Präferenzen bei der Gewichtungsverteilung der Kriterien in der Excel-Tabelle flexibel abgebildet werden können, ohne weitere Anpassungen vornehmen zu müssen.

Von den Verfassern wurde eine beispielhafte Gewichtung definiert, um im weiteren Verlauf dieser Arbeit eine Bewertung der ausgewählten CMS vornehmen zu können. Die Gewichtungsverteilung erfolgte über ein schrittweises Vorgehen. Dabei wurden vom Groben bis ins Detail, von der Kategorie bis hin zum jeweiligen Kriterium, Prozentwerte vergeben. In der Excel-Tabelle welche auf der beiliegenden CD enthalten ist, ist eine beispielhafte Gewichtung angegeben.

5.2 Maximale Scores angeben

Um in der vierten Spalte des Bewertungsrasters die maximalen Scores berechnen zu können, wird grundlegend die folgende Formel verwendet:

$$\text{max. Scores} = (\text{Kategoriegewichtung} * \text{Unterkategoriegewichtung} * \text{Kriteriengewichtung}) * 100$$

Die maximalen Scores errechnen sich anhand der vom Entscheidungsträger festgelegten Gewichtung der Kategorien, Unterkategorien und Kriterien in Prozentwerten. Diese werden miteinander multipliziert und schlussendlich mit 100 multipliziert. Daraus ergeben sich die maximalen Scores pro Kriterium, welche zugleich ebenso die Gewichtung des Kriteriums am Gesamtziel darstellen. Um dies zu verdeutlichen dient das folgende Beispiel:

Die Oberkategorie ‚CMS allgemein' erhält die Gewichtung 33,3% (0,333), die Unterkategorie ‚Erweiterbarkeit' wird mit 30% (0,300) gewichtet. Das konkrete Kriterium 'durch Plugins' soll mit 50% (0,5) innerhalb der Unterkategorie bewertet werden. Eingetragen in die Formel ergibt sich: (0,333 * 0,3 * 0,5) * 100 = 5 Es können maximal 5 Scores erreicht werden.

Entstandene Sonderfälle ist hierbei das Kriterium ‚Barrierefreiheit' sowie die Unterkategorie ‚redaktioneller Freigabeprozess. Hierbei wird für die ‚Barrierefreiheit' in der Formel eine weiteres Gewichtungselement hinzugefügt, da in einer weiteren Ebene zwischen Besucher und Entwickler unterschieden werden kann. Beim ‚redaktionellen Freigabeprozess' hingegen entfällt eine Ebene der Gewichtung, da hier nicht weiter differenziert werden kann. Diese beiden Sonderfälle können der Excel-Tabelle auf der beiliegenden CD entnommen werden.

Somit sind die Bestandteile des Bewertungsrasters von CMS Systemen beschrieben, welche die linke Seite der Excel-Tabelle darstellt. In den folgenden beiden Kapiteln erfolgt eine Darstellung der Bestandteile der CMS Bewertung (rechte Seite der Excel-Tabelle).

5.3 Bewertungsskala definieren

Eine Bewertungsskala muss aufgestellt werden, um zu dokumentieren in welchem Maße ein Kriterium erfüllt ist. Hierfür wird eine ordinale Bewertungsskala über Punktwerte verwendet, da nicht alle Kriterien in Zahlen messbar sind. Die Bewertungsskala reicht von 0 Punktwerte (sehr schlecht) bis 5 Punktwerte (sehr gut). Diese Skala ist in Tab. 2 abgebildet.

Bewertung	Punktwert
Sehr gut	5
Gut	4
Eher gut	3
Eher schlecht	2
Schlecht	1
Sehr schlecht	0

Tab 2: Ordinale Bewertungsskala des Erreichungsgrades der Kriterien

Diese Punktwerte werden im rechten Bereich der Excel-Tabelle, der CMS Bewertung, in der zweiten Spalte (‚Bewertung') eines jeden Systems eingetragen. Vorangehend sind in der ersten Spalte Kommentare oder auch festgelegte Vorgaben einzutragen, um eine Grundlage für die Bewertung zu geben oder sie nachvollziehen zu können. Abb. 8 veranschaulicht diese Aufteilung. In der dritten und letzten Spalte (‚Scores') der CMS Bewertung errechnen sich dabei die jeweiligen Scores für ein Kriterium eines CMS. Über welche Formel dies genau erfolgt wird in Kapitel 5.4 erläutert.

CMS Bewertung								
Joomla!			TYPO3			Drupal		
Vorgabe/ Kommentar	Bewer-tung	Scores	Vorgabe/ Kommentar	Bewer-tung	Scores	Vorgabe/ Kommentar	Bewer-tung	Scores

Abb. 8: Aufteilung innerhalb der Bewertung der jeweiligen CMS

Die Skalenbreite von 0-5 Punktwerten wurde gewählt, um den Erreichungsgrad aussagekräftig zu differenzieren. Dabei sollte die Breite der Skala gleichzeitig nicht zu groß sein, damit ein Verständnis für die Bedeutung der einzelnen Punktwerte erhalten bleibt. Sechs verschiedene Punktwerte haben den Vorteil, dass es keinen Mittelwert gibt. Somit wird bewusst gefordert, eine eher positive oder negative Bewertung zu geben, um letztendlich eine deutliche Aussagekraft zu erreichen. Um auf den ersten Blick unmissverständlich erkennen zu können, welche Kriterien in welchem Maße erfüllt sind, verdeutlicht eine farbliche Formatierung in der Excel-Tabelle die Bewertung. Damit die Übersichtlichkeit bewahrt bleibt, wurden drei

Farbcluster gebildet. Grün soll bei der Bewertung eine hohe Punktzahl verdeutlichen und lässt sich als Stärke interpretieren. Die Farbe Gelb symbolisiert eine mittlere Punktzahl. Eine geringe Punktzahl bei der Bewertung wird mit der Farbe Rot visualisiert und lässt sich als Schwäche auslegen.

Bei der Bewertung sind grundsätzlich quantitative und qualitative Kriterien zu unterscheiden. Für quantitativ messbaren Kriterien wird vorgeschlagen, die Bewertungsskala nach dem Rangordnungsprinzip anzuwenden. Qualitative Merkmale können je nach Ausprägung eines einzelnen Kriteriums mit den Punktwerten von 0-5 bewertet werden. Beispielsweise kann bei der Prüfung, auf das Vorhandensein eines Versionsmanagements festgestellt werden, ob dieses bereits integriert ist (5 Punktwerte), durch eine Erweiterung hinzugefügt werden kann (3 Punktwerte) oder nicht existiert (0 Punktwerte). Die jeweilige Punktevergabe obliegt jedoch dem jeweiligen Benutzer.

5.4 Scores berechnen

Um in der dritten Spalte der CMS Bewertung die Scores zu berechnen, wird die folgende Formel verwendet:

$$\text{erreichte Scores} = \text{max. Scores} * \frac{\text{erhaltene Bewertung}}{\text{max. Bewertung}}$$

Die erreichten Scores je Kriterium errechnen sich aus den maximal zu vergebenden Scores multipliziert mit dem Verhältnis von der erhaltenen zur maximalen Bewertung (Punktwert). Wie bereits erwähnt, bringt die Verwendung dieser Formel den Vorteil mit sich, dass die in der Excel-Tabelle eingetragene Gewichtung unabhängig von der Berechnung der Scores verändert werden kann. Ein Beispiel für die Berechnung von erreichten Scores ist das Folgende:

Das Kriterium ‚Erweiterbarkeit durch Plugins', der Oberkategorie ‚CMS allgemein' besitzt maximale Scores von 5. In der Bewertung erhielt es 4 Punktwerte. Wie im vorherigen Kapitel beschreiben kann maximal die Bewertung mit 5 Punktwerten erfolgen. Daraus ergibt sich für die erreichten Scores das folgende Ergebnis: 5 * 4/5 = 4 Das Kriterium ‚Erweiterbarkeit durch Plugins' erreichte 4 Scores.

Somit sind die Vorarbeiten für die Bewertung von CMS abgeschlossen und es kann ein Marktüberblick über die bestehenden CMS gegeben werden. Auf dieser Grundlage erfolgt die Durchführung der Untersuchung von ausgewählten CMS.

6 Marktübersicht

Um einen Überblick über den Markt von OS CMS zu bekommen wurde grundlegende Recherche betrieben. Alle identifizierten Systeme wurden aufgelistet, wie in Anhang 3 zu sehen ist. Als Grundlage diente hierfür www.ohloh.net und www.github.com sowie die jeweilige Website des Systems. Es wurden insgesamt 111 CMS identifiziert. Im weiteren Schritt wurden alle diese Systeme auf festgelegte Mindestvoraussetzungen überprüft, welche als KO-Kriterien dienten. Hierfür wurden aus den bestehenden 98 Kriterien die folgenden zwei Kriterien als Mindestvoraussetzung festgelegt. Das CMS muss mehr als 5 Entwickler besitzen und die letzte Aktualisierung darf nicht länger als 1 Jahr zurück liegen. Diese beiden Kriterien, sind Abb. 9 zu entnehmen. Sie sollten alle Systeme eliminieren, welche sich nicht für den Einsatz für großen Unternehmen eigenen, da sie keiner großen Weiterentwicklung erfahren und nicht aktuell gehalten werden.

Abb. 9: Mindestvoraussetzungen (KO-Kriterien) für OS CMS

Rot markiert sind in Anhang 3 die Systeme, die diese Mindestvoraussetzungen nicht erfüllen. Schwarz markierte Systeme erfüllen dahingegen diese beiden zunächst definierten Mindestanforderungen. Dies betrifft 43 CMS. Diese Systeme wurden im folgenden Schritt weitergehend analysiert.

6.1 Detailliertere Marktanalyse

Die verbleibenden 43 Systeme wurden anhand der folgenden vier Kriterien weiterhin untersucht, um ihre Relevanz für den Einsatz in großen Unternehmen festzustellen.

- Anzahl der Entwickler
- Produktalter des CMS
- Veröffentlichungshäufigkeit von Aktualisierungen
- Vorhandensein eines Rollenkonzepts
- Unterstützung von Staging

Diese Analyse stellte sich als sehr zeitintensiv heraus, wobei sich herausstellte, dass nur sehr wenige Systeme kein Rollenkonzept besitzen. Bei der Recherche konnte bei keinem der Systeme festgestellt werden, ob es Staging unterstützt. Diese Angabe wurde in keinem Featurekatalog angegeben oder war mit nur wenig Aufwand herauszufinden. Daher wurde nach der Untersuchung von 24 Systemen die weitere Analyse abgebrochen. Die Ergebnisse, die bis zu diesem Zeitpunkt erforscht wurden, sind in Anhang 4 beigefügt.

Als Alternative zu dieser Vorgehensweise sollte eine aktuelle Momentaufnahme der Relevanz der CMS erfolgen. Dafür sollte über Google Trends identifiziert werden, wie hoch die Anzahl der Suchanfragen zu dem jeweiligen CMS ist. Diese Ergebnisse sollten als Indikator für die Relevanz der Systeme am Markt dienen. Bei der Recherche wurde festgestellt, dass dies nicht zielführend ist. Zur Veranschaulichung dient hierfür das folgende Beispiel. Wie in Abb. 10 zu sehen ist, wurde laut Google Trends nach Joomla! um ein Vielfaches mehr gesucht als beispielsweise nach den Systemen Typo3 oder SilverStripe.

Abb. 10: Suchvolumen in Google nach beispielhaften CMS[30]

Bei der genaueren Betrachtung lässt sich jedoch feststellen, dass die Suchanfragen zu Joomla! zum größten Teil aus Ländern wie Kuba, Mongolei oder Kamerun kommen. Dabei ist in Kuba das Internet verboten und es ist somit fraglich woher die zahlreichen Suchanfra-

[30] Enthalten in: Google (2014)

gen stammen. In Abb. 11 ist dies zur Verdeutlichung noch einmal dargestellt. Ähnliche Ergebnisse wurden auch bei anderen CMS erzielt.

Regionales Interesse

joomla typo3 silverstripe

Region | Stadt

Region	Wert
Kuba	100
Mongolei	46
Kamerun	45
Madagaskar	41
Benin	40
Togo	36
Kenia	35

Abb. 11: Regionale Verteilung des Suchvolumens nach Joomla! in Google[31]

Dabei haben sich die gesuchten Begriffe in Kombination mit Joomla! ständig auf das CMS bezogen. Dies ist beispielsweise durch die Angabe der Versionsnummer oder den Begrifflichkeiten ‚template' und ‚download' zu sehen, wie in Abb. 12 dargestellt. Schlussendlich wurde diese Betrachtungsweise als nicht aussagekräftig und standhaft angesehen.

Suchanfragen	Beliebteste Zunehmen...
joomla template	100
template	95
templates joomla	80
templates	80
joomla 1.5	75
joomla 2.5	60
joomla download	55

Einbetten

Abb. 12: Beliebte Suchanfragen in Verbindung mit Joomla![32]

[31] Enthalten in: Google (2014)
[32] Enthalten in: Ebenda

6.2 Marktanteile

Um die Relevanz der verschiedenen CMS am Markt abzubilden wurde letztendlich auf den Marktanteil zurückgegriffen. Dieser wurde aus zwei Gesichtspunkten betrachtet. Zum einen aus der Sicht aus Deutschland, Österreich und der Schweiz, wie in Abb. 13 zu sehen ist. Interessant wäre dabei die Unterscheidung in private und gewerbliche Nutzung. Darüber gibt es jedoch leider getrennten Statistiken. Die beiden Bereiche werden ausschließlich zusammengefasst betrachtet. Hierbei zeichnet sich Wordpress als das populärste System aus. Daraufhin folgen anhand der Verbreitung Joomla!, TYPO3, Contao, Drupal und Magento. Die verbleibenden 13% teilen sich auf zahlreiche CMS auf, die in Deutschland, Österreich und der Schweiz auf nicht mehr als 1% Marktanteil kommen.

Abb. 13: Marktanteile der OS CMS in Deutschland, Österreich und der Schweiz[33]

Zum anderen verteilt sich der weltweite Marktanteil der CMS folgendermaßen. Wordpress ist auch weltweit gesehen das mit Abstand verbreitetste CMS. Danach folgen aus weltweiter Sicht Joomla!, Drupal, Magento und TYPO3. Viele weitere CMS teilen sich stark verstreut die restlichen 18 % des Gesamtmarktes. Diese Verteilung des weltweiten Marktanteils ist in Abb. 14 dargestellt.

[33] Mit Änderungen entnommen aus: Webkalkulator (o. J.a)

Marktanteil (weltweit)

21%
2%
3%
5%
9%
60%

Wordpress Joomla! Drupal Magento TYPO3 Sonstige

Abb. 14: Marktanteil der OS CMS weltweit[34]

Anhand dieser beiden Statistiken zum Marktanteil der CMS sowie der in Anhang X beigefügten Liste der existierenden CMS wurde eine Auswahl für die exemplarische Untersuchung der CMS getroffen. Wordpress wurde nicht betrachtet, da dieses speziell zur Veröffentlichung von Content im Blogsystem konzipiert wurde.[35] Der Fokus liegt eindeutig im Erstellen und Verwalten von Blogs, was sich für den Unternehmenseinsatz nicht eignet.[36] Schlussendlich sollen Joomla!, TYPO3, Contao, Drupal und Plone als beispielhafte prominente Repräsentanten von CMS genauer untersucht werden.

6.3 CMS Installation

Die Systeme wurden auf einem Computer mit dem Betriebssystem Windows 7 durchgeführt. Als HTTP-Server kam Apache zum Einsatz sowie die Datenbank MySQL. Als Browser wurde Mozilla Firefox in der Version 26 verwendet. Zur Bereitstellung des Servers und der Datenbank wurde die Anwendung XAMPP eingesetzt.

Um die CMS Joomla!, TYPO3 und Drupal installieren zu können, mussten diese zunächst in den Ordner htdocs der Anwendung XAMPP verschoben werden. Dies war notwendig da die Systeme keine direkt ausführbare Installationsdatei besitzen, sondern die Installation bei allen drei Systemen php-gestützt war. Die Installation konnte durch Eingabe der Adresse ‘localhost/*Bezeichnung des Systems*‘ in die Navigationsleiste des Browser gestartet werden.

[34] Mit Änderungen entnommen aus: W3Techs (2014)
[35] Vgl. Diehl, A. (o. J.)
[36] Vgl. Wordpress (o. J.)

Als erstes System wurde Joomla! in der Version 3.2.1 installiert. Die Installation war hierbei recht intuitiv. Der Anwender wird Schritt für Schritt durch die einzelnen Konfigurationsmasken geleitet. Der komplette Installationsprozess dauert hierbei nicht mal eine Minute. Bei der Testinstallation traten keinerlei Probleme oder Fehler auf. Nach der Installation muss beachtet werden, dass ein Ordner manuell gelöscht werden muss, um den Prozess erfolgreich abschließen zu können.

Anschließend wurde das CMS TYPO3 in der Version 6.1.7 installiert. Der Installationsvorgang war hierbei ebenfalls sehr intuitiv und übersichtlich. Allerdings traten während des Installationsprozesses diverse Fehler auf, obwohl dieselbe Konfigurationen wie unter Joomla! verwendet wurden. Nachdem der Installationsvorgang fehlerhaft war, muss der Ordner aus htdocs komplett gelöscht und erneut im Originalzustand hineinkopiert werden, da ansonsten jedes Mal beim Versuch das System Aufzurufen zu Fehlermeldung der Installation angezeigt wird. Nach ungefähr drei bis vier Fehlversuchen funktionierte die Installation unter veränderten Konfigurationseinstellungen.

Im Anschluss daran wurde das dritte CMS Drupal in der Version 7.25 installiert. Auch bei diesem System war die Navigation durch die Installation äußerst unkompliziert. Nach vier Konfigurationsseiten begann der Installationsprozess. Allerdings traten auch bei dieser Installation Fehler auf. Nachdem die Originaldaten widerhergestellt wurden, konnte die Installation im zweiten Versuch erfolgreich durchgeführt werden.

Danach waren die drei relevanten Systeme installiert und konnte näher untersucht werden. An dieser Stelle ist wichtig zu erwähnen, dass zusätzlich das System SilverStripe installiert wurde. Aus Kapazitätsengpässen wurde sich allerdings gegen eine nähere Untersuchung entschieden. Ferner standen während der Entscheidungsphase welche Systeme näher untersucht werden sollen die Systeme Plone und Contao in der näheren Auswahl.

Das Problem bei Plone bestand zum einen darin, dass die aktuellste Version noch nicht für Windows verfügbar war. Zum anderen gab es Probleme bei der Installation der Vorversion. So konnte diese aus bislang nicht bekannten Gründen nicht zum Laufen gebracht werden.

Bei Contao gab es ebenfalls Probleme bei der Installation. Nachdem alle Installationsversuche fehlgeschlagen sind, wurde versucht mit der Überprüfung durch Contao Check 7.9 zu ermitteln, weshalb die Installation nicht möglich war. Das Ergebnis ist in Abb. 15 dargestellt. So gab es Probleme bei der Verwendung des Live Updates, da der Server nicht erreicht werden kann.

Abb. 15: Installationsfehler bei Contao

Auf Grund der oben genannten Probleme wurde entschieden neben Joomla! und Typo3 das CMS Drupal im Rahmen dieser Arbeit näher zu betrachten. Alle installierten Systeme sind zudem zusammen mit dem Kriterienkatalog auf dem beigelegten Datenträger zu finden.

7 Untersuchung ausgewählter CMS

Im Rahmen dieses Kapitels soll zunächst eine Beschreibung der ausgewählten Systeme erfolgen. Im Anschluss daran erfolgt eine Beschreibung der durchgeführten Nutzwertanalyse und beschrieben, wie sich das Ergebnis der Analyse exakt zusammensetzt.

7.1 Joomla!

Joomla bedeutet übersetzt so viel wie „alle zusammen" und stellt ein OS CMS Projekt dar. Die Entwickler von Joomla! publizieren das System grundsätzlich unter der General Public Licence (GPL-Lizenz). Das hat zur Folge, dass die Rechte für die freie Nutzung und insbesondere Veränderungen des Quellcodes weitergeben werden. Das System steht somit kostenfrei zur Verfügung. Joomla! 1.0 wurde am 1. September 2005 veröffentlicht. Das System basiert allerdings auf dem CMS Mambo, welches bereits im Jahr 2000 veröffentlicht wurde. [37] Der Marktanteil von Joomla! beträgt im deutschsprachigen Raum derzeit ca. 23 %.[38]

„Das CMS basiert auf der weit verbreiteten und bewährten Kombination aus der Programmiersprache PHP und dem Datenbanksystem MySQL." [39] Das System lässt sich darüber hinaus selbst von unerfahrenen Anwendern ohne größeren Aufwand und Vorkenntnisse installieren und vorkonfigurieren. Darüber hinaus wird von einigen Hosting-Anbietern auch eine Ein-Klick-Installation angeboten. Durch die einfache Art und Weise Joomla! lauffähig zu bekommen, lässt sich eine einfache Seite bereits in weniger als fünf Minuten erstellen. Das System wird in über 60 Sprachen angeboten und Unterstützt darüber hinaus die Verwaltung von mehrsprachigen Content, was die Voraussetzung für einen globalen Einsatz darstellt.[40]

Im Folgenden sollen der Datenaustausch sowie die Kommunikation der einzelnen Komponenten von Joomla! näher erläutert werden. Der prinzipielle Ablauf ist hierbei bei jedem untersuchten CMS äquivalent.

Nachdem Joomla! über den Browser aufgerufen wird, kann das System direkt vom Client aus verwendet werden. Hierbei schickt der Client eine Anfrage an den Webserver wie z.B. Apache, welcher die Anfrage entgegennimmt und verarbeitet. Je nachdem welcher Inhalt von dem Client angefordert wird, schickt der Server eine entsprechende HTML-Seite aus dem Frontend oder eine Oberfläche des Backends an den Client zurück. Das Resultat wird dort im Browser angezeigt.[41] Bei einer Webapplikation wie Joomla! kann der Server anhand der Endung „.php" erkennen, dass es sich um ein Skript handelt, welches gesondert ausge-

[37] Vgl. Kempkens, A., (2009), S. 29 ff.
[38] Vgl. Webkalkulator (o. J.b)
[39] Joomla! (o. J.)
[40] Vgl. ebenda
[41] Vgl. Ebersbach, A./Glaser, M./Kubani, R. (2009), S. 40 f.

führt werden muss. Das bedeutet, dass Joomla! gestartet wird und damit die Verarbeitung durch das CMS. Abschließend werden diverse Prüfungen vorgenommen um die angeforderte Seite fehlerfrei aus den einzelnen Komponenten zusammenbauen zu können. Die einzelnen Komponenten werden hierbei von Joomla selbst erstellt.[42]

In der Abb. 16 ist zu erkennen, dass die angefragten Inhalte aus einer MySQL-Datenbank geholt und anschließend an der richtigen Stelle einer bestimmten HTML-Vorlage eingebaut werden. Joomla! ist hierbei durch Ausführung eines bestimmten PHP-Skriptes für den korrekten Aufbau der HTML-Seite verantwortlich Wenn der komplette HTML-Code erzeugt ist, wird die Seite an den Webserver übergeben, welcher sie dann an den Client sendet.

Abb. 16: Technischer Datenaustausch zwischen den einzelnen Komponenten[43]

Joomla bietet etliche Funktionen die von einem modernen CMS erwartet werden. Das CMS wird als äußerst flexibel und anpassbar angepriesen und bietet eine sehr große Community. Neue Version erscheinen bei diesem System im Halbjahresrhythmus. Problematisch gestaltet sich hingegen die Administration von Websites da das Administrationspanel sehr schwer zu durschauen ist. Zudem sind längst nicht alle Funktionalitäten voll ausgereift. [44] Was das System im Vergleich zu TYPO3 und Drupal leisten kann und worin seine Schwächen bestehen, wird der Vergleichstest zeigen, welcher in Kapitel 7.4 näher erläutert wird.

Um einen Einblick in das CMS Joomla! zu bekommen, ist in Abb. 17 zur Veranschaulichung ein Screenshot des Systems dargestellt.

[42] Vgl. Ebersbach, A./Glaser, M./Kubani, R. (2009), S. 40 f.
[43] Enthalten in: Ebenda
[44] Vgl. Webkalkulator (o. J.b)

Abb. 17: Screenshot des Startbildschirms von Joomla!

Die obige Abb. 17 zeigt den Hauptbildschirm des CMS Joomla! nach Anmeldung als Administrator. In der obersten Zeile sowie in der linken Spalte befindet sich der Navigationsbereich. In dem mittleren Bereich werden hierbei aktuelle Informationen angezeigt.

7.2 TYPO3

TYPO3 ist ein von Kasper Skårhøj entwickeltes OS CMS, welcher im Jahr 1997 mit der Entwicklung begann.[45] Der Name TYPO3 stammt von Tippfehler (*typing error*, abgekürzt *typo*). Kasper Skårhøj verlor durch einen Tippfehler einen Bestandteil seiner Arbeit, wonach er das System benannte. Die Zahl *3* wurde angehängt, da die dritte Version des Systems, welche 2001 veröffentlicht wurde, den ersten Erfolg brachte.[46]

TYPO3 ist ein frei konfigurierbares CMS, das für die Pflege von dynamisch generierten Internetpräsentationen verwendet wird. Dieses CMS hat in den letzten Jahren immer mehr an Bedeutung gewonnen. Außerdem wurde das System unter der GPL-Lizenz publiziert. Somit stellt TYPO3 ebenfalls keine kostenpflichtige Software dar. Bei der Auswahl eines CMS stehen für viele Privatanwender die Kosten im Vordergrund. Unternehmen schätzen hingegen an TYPO3 insbesondere die Leistungsfähigkeit, Stabilität und Flexibilität.[47]

Das System zeichnet sich vor allem durch die umfangreiche Kompatibilität aus. So kann es auf allen gängigen Betriebssystemen wie z. B. Microsoft Windows, Macintosh OSX oder Linux betrieben werden. Darüber hinaus können unterschiedliche Webserver verwendet werden, wie beispielsweise Microsoft IIS oder Apache. TYPO3 wurde auf einem sogenannten LAMP-System (Linux, Apache, MySQL, PHP) entwickelt und so wird Linux auch als Betriebssystem empfohlen, da es darauf die höchste Performance aufweist. Eine wichtige Voraussetzung für den Einsatz vom TYPO3 ist PHP, da das System auf dieser Skriptsprache basiert.[48] Zusammen mit WordPress, Joomla! und Drupal und Contao gehört es zu den bekanntesten CMS im OS Bereich. Aktuell beträgt der Marktanteil von TYPO 3 in Deutschland, Österreich und der Schweiz ca. 14%.[49]

Um ebenfalls einen Einblick in das CMS TYPO3 zu erhalten, ist in Abb. 18 zur Veranschaulichung ein Screenshot des Systems dargestellt.

[45] Vgl. TYPO3 (o. J.a)
[46] Vgl. TYPO3 (o. J.b)
[47] Vgl. Meyer, R. (2013), S. 1
[48] Vgl. TYPO3 (o. J.c)
[49] Vgl. Webkalkulator (o. J.b)

Abb. 18: Screenshot des Startbildschirms von TYPO3

Nach Anmeldung an das System als Administrator, erscheint die oben gezeigte Maske auf dem Bildschirm. Im Vergleich zu Joomla! befindet sich bei TYPO3 die Navigationsleiste komplett in der linken Spalte. Die Anzeige ist hierbei dreigeteilt. Ganz links befindet sich die Navigation, in der Mitte werden die einzelnen Websites dargestellt und in der rechten Spalte wird der eigentliche Inhalt angezeigt.

7.3 Drupal

Drupal wurde von Dries Buytaert am 15. Januar 2001 unter der Bezeichnung drop.org entwickelt. Die Idee war, Anwendern die Möglichkeit zu geben, die Software selbst auszuprobieren, diese zu erweitern und weiterzuentwickeln.[50] Drupal ist ein freies CMS, mit Hilfe dessen sich Webauftritte verschiedener Ausrichtungen komfortabel aufgesetzt und gepflegt werden können. Das System steht ebenfalls unter der GNU GPL Lizenzierung, d.h. dass für die Nutzung dieser Software keine Lizenzkosten bezahlt werden müssen. Außerdem gewährleistet eine große Community die Weiterentwicklung des Systems und seiner Erweiterungen.[51]

Darüber hinaus ist Drupal eine dynamische Webanwendung. Es setzt sich aus einer Reihe von Komponenten, die in der Programmiersprache PHP implementiert sind, zusammen. Für den Einsatz wird wie bei den beiden anderen beschrieben CMS ein Webserver vorausgesetzt sowie eine Datenbank für die Ablage der Daten. Der Zugang zu den Administrations-, Konfigurations-, und Redaktionsbereichen der jeweiligen Seite ist ebenfalls über das System selbst möglich.[52]

Drupal kann wie Joomla! und TYPO3 leicht installiert und konfiguriert werden. Allerdings wird generell empfohlen, dass ein Grundverständnis von Programmierung und den zugrundeliegende Internettechniken bei komplizierten Aktionen vorhanden ist. Bei Fragen kann sich der Anwender jederzeit Hilfestellung in den offiziellen Foren holen.[53] Für die Verwendung von Drupal wird kein bestimmtes Betriebssystem vorausgesetzt. Das CMS ist sowohl auf Microsoft Windows, Macintosh OSC als auch auf Linux lauffähig.[54] Derzeit beträgt der Marktanteil von Drupal im deutschsprachigen Raum 4 %.[55]

Drupal ermöglicht es einem oder auch mehrere Anwendern wie jedes andere CMS ebenfalls Inhalte auf Websites zu veröffentlichen sowie diese zu verwalten und zu organisieren. Nachfolgend ist eine beispielhafte Auflistung der verschiedenen Einsatzgebiete eines CMS dargestellt:

- Webbasierte Community Portale
- Firmenwebsites
- Private Websites oder Weblogs
- E-Commerce-Anwendungen
- Informationsverzeichnisse[56]

[50] Graf, H. (2008), S. 31
[51] Vgl. Stahl, F./Schettler, O. (2012), S. 1
[52] Vgl. Stahl, F./Schettler, O. (2012), S. 9
[53] Vgl. Luhm, T. (2011), S. 13 f.
[54] Vgl. ebenda, S. 17
[55] Vgl. Webkalkulator (o. J. b)
[56] Vgl. Graf, H. (2008), S. 25 f.

Um auch einen Einblick in das CMS Drupal zu erhalten, ist in nachfolgender Abb. 19 zur Veranschaulichung ein Screenshot des Systems zu sehen.

Abb. 19: Screenshot des Startbildschirms von Drupal

Drupal unterscheidet sich deutlich vom Erscheinungsbild nach erfolgter Anmeldung. Die Startseite erscheint recht schlicht. So lässt sich direkt die Navigation oder der Inhalt anpassen. Es besteht zudem die Möglichkeit direkt zum Administrationsbereich zu gelangen.

7.4 Ergebnisse der Nutzwertanalyse

Nachfolgend werden die Ergebnisse ausgewählter Unterkategorien und Kriterien zu den drei untersuchten Systemen vorgestellt und beschrieben durch welche Stärken und Schwächen sich die Systeme jeweils auszeichnen.

7.4.1 Joomla!

CMS allgemein

Erweiterbarkeit:

Das CMS lässt sich sowohl durch Plugins, Module als auch durch Portlets erweitern. Lediglich die im Vergleich zu Drupal geringere Anzahl von angebotenen Plugins führt zu Abzügen.

Funktionalitäten:

Rücksicherungen sind ohne Probleme möglich. Zudem bietet das System eine interne Suche mit integrierter Anfertigung einer Suchstatistik an. Für den Im- und Export von Inhalten steht eine XML-RPC Schnittstelle zur Verfügung. Einzig die Möglichkeit einzelne Bereiche rückzusichern wird bei Joomla! vermisst.

Kompatibilität:

Die Anwendung ist mit HTML5 kompatibel. Weiter wird das Responsive Webdesign vollumfänglich unterstützt. Darüber hinaus läuft das System auf allen Browsern, die CSS unterstützen. In dieser Kategorie werden alle Kriterien zur vollsten Zufriedenheit erfüllt.

Unternehmenseinsatz

Plattformunabhängigkeit:

Joomla! unterstützt die Webserver Apache, Nginx und Microsoft ISS. Als Datenbanken können MySQL, Microsoft SQL und PostgreSQL verwendet werden. Zudem werden die Skriptsprachen PHP und JavaScript unterstützt. Die Software-Entwicklung folgt dem Model-View-Controller-Konzept. Einzig die vermissende Kompatibilität zu Oracle-Datenbanken ergab Abzüge in dieser Kategorie. Als Betriebssystem werden Linux, Microsoft Windows und Macintosh OSX unterstützt.

Berechtigung innerhalb des Systems:

Eine automatische Berechtigungszuweisung ist durch eine Schnittstelle zu einem LDAP-Server über eine Erweiterung möglich. Zudem besteht ein die Möglichkeit Benutzerrollen anzulegen und zu verwalten sowie Benutzerberechtigungen zu vererben. Einzig die Mandantenunterstützung gibt Anlass zur Beanstandung. Diese ist lediglich durch eine Erweiterung möglich, die zudem auf jeder Seite installiert werden muss, wo diese benötigt wird.

Aufwand:

Das System konnte intuitiv und ohne Auftreten von Fehlern installiert werden. Updates lassen sich allerdings nicht automatisiert durchführen. Diese müssen manuell von Experten vorgenommen werden.

Templateverwaltung/ -erstellung:

Es ist möglich sowohl von Websites als auch von Content Vorlagen zu erstellen und diese zu verwalten.

Open Source

Community:

Mit einer Größe von rund 550.000 Mitgliedern ist die Community von Joomla! die zweitgrößte hinter Drupal. Die Summe aller Forenbeiträge ist allerdings mit ca. 3 Millionen weit vor denen der untersuchten Konkurrenzsysteme.

Dokumentation:

Bei den Dokumentationen gibt sich Joomla! keine Blöße. Neben einer Codedokumentation, einem Benutzer- und Entwicklerhandbuch ist sogar ein FAQ vorhanden. Die Dokumentationen sind derzeit allerdings nur auf Englisch vorhanden.

Verbreitungsgrad:

Mit rund 15 Millionen Downloads und 221 Entwickler ist Joomla! weit vor Typo3 und Drupal.

Support:

Für das System sind etliche hilfreiche Tutorials vorhanden. Allerdings steht lediglich ein veraltetes Wiki von einem externen Anbieter zur Verfügung. Zudem gibt es nur sehr eingeschränkten Support durch Dienstleister für dieses System.

Sonstige:

Das System unterstützt derzeit über 60 unterschiedliche Sprachen. Mit rund 2,8 Millionen Websites die auf Basis von Joomla erstellt wurden, führt Joomla! derzeit den Vergleich mit den anderen Systemen klar an. Der Marktanteil im deutschsprachigen Raum beträgt aktuell 23%. Das System ist mit einem Produktalter von neun Jahren allerdings das jüngste der drei untersuchten Systeme.

7.4.2 TYPO3

CMS allgemein

Erweiterbarkeit:

Das CMS lässt sich ebenfalls sowohl durch Plugins, Module als auch durch Portlets erweitern. Im Vergleich zu den anderen beiden Systemen bietet es allerdings mit rund 5.000 Plugins den geringsten Wert.

Funktionalitäten:

Rücksicherungen sind auch hier ohne Probleme möglich. Eine interne Suche ist ebenfalls möglich. Für den Im- und Export von Inhalten steht eine XML-RPC Schnittstelle zur Verfügung. Auch hier ist anzumerken, dass die Möglichkeit einzelne Bereiche rücksichern zu können vermisst wird. Zudem ist keine automatisch erstellte Suchstatistik vorhanden.

Kompatibilität:

Die Anwendung ist mit HTML5 kompatibel. Weiter wird das Responsive Webdesign vollumfänglich unterstützt. Darüber hinaus läuft das System auf allen gängigen Browsern wie Internet Explorer, Firefox oder Opera. In dieser Kategorie werden wie auch bei Joomla! alle Kriterien zur vollsten Zufriedenheit erfüllt.

Unternehmenseinsatz

Plattformunabhängigkeit:

Joomla! unterstützt die Webserver Apache und Microsoft ISS. Als Datenbanken können MySQL, PostgreSQL und Oracle verwendet werden. Zudem werden die Skriptsprachen PHP und JavaScript unterstützt. Die Software-Entwicklung folgt dem Model-View-Controller-Konzept. Als Betriebssystem werden Linux, Microsoft Windows und Macintosh OSX unterstützt.

Berechtigung innerhalb des Systems:

TYPO3 bietet als einziges eine problemlose Mandantenunterstützung. Eine automatische Berechtigungszuweisung durch eine Schnittstelle zu einem LDAP-Server über eine Erweiterung ist ebenfalls möglich. Zudem besteht ein die Möglichkeit Benutzerrollen anzulegen und zu verwalten. Einzig die Möglichkeit Benutzerberechtigungen zu vererben wird hier nicht möglich.

Aufwand:

Die Installation war intuitiv gestaltet. Allerdings traten einige Fehler bei der Installation auf, sodass sich diese sehr zeitaufwändig gestaltet hat. Updates lassen sich ebenfalls nicht au-

tomatisiert durchführen. Diese müssen auch hier manuell von Experten vorgenommen werden.

Templateverwaltung/ -erstellung:

Typo3 setzt bei der Erstellung von Templates auf eine eigene Templateengine. Dies ist im Vergleich zu den anderen beiden Systemen positiv hervorzuheben. Eine Verwaltung von Templates ist ebenfalls möglich.

Open Source

Community:

Mit einer Größe von rund 110.000 Mitgliedern ist die Community von TYPO3 deutlich die kleinste. Die Summe aller Forenbeiträge beläuft sich auf rund 0,6 Millionen und ist somit ebenfalls der geringste Wert im Vergleich zu den beiden anderen Konkurrenzsystemen.

Dokumentation:

Bei den Dokumentationen gibt sich Typo3 ebenfalls keine Blöße. Neben einer Codedokumentation, einem Benutzer- und Entwicklerhandbuch ist auch hier ein FAQ vorhanden. Die Dokumentationen sind neben Englisch noch auf Russisch vorhanden.

Verbreitungsgrad:

Mit rund sechs Millionen Downloads und 155 Entwickler nimmt TYPO3 hinter Joomla! den zweiten Rang ein.

Support:

Der Support ist bei TYPO3 vorbildlich. Neben einem Dienstleister als Ansprechpartner gibt er ein Wiki für Selbstsupport sowie Video-Tutorials.

Sonstige:

Das System unterstützt derzeit über 50 unterschiedliche Sprachen und belegt somit den dritten und letzten Rang. Mit rund 366 Tausend Websites die auf Basis von TYPO3 erstellt wurden, belegt das System auch hier den letzten Rang. Der Marktanteil im deutschsprachigen Raum beträgt aktuell 14%. Das System ist mit einem Produktalter von 16 Jahren das älteste der drei untersuchten Systeme.

7.4.3 Drupal

CMS allgemein

Erweiterbarkeit:

Das CMS lässt sich sowohl durch Plugins, Module als auch durch Portlets erweitern. Es bietet mit 14.000 Plugins die größte Anzahl an Erweiterungen. Allerdings bestehen zwischen einzelnen Modulen und Versionen zahlreiche Abhängigkeiten.

Funktionalitäten:

Rücksicherungen sind ohne Probleme möglich. Darüber hinaus lassen sich sogar einzelne Bereiche rücksichern. Ferner bietet das System eine integrierte interne Suche. Für den Im- und Export von Inhalten fehlt allerdings jegliche Schnittstelle.

Kompatibilität:

Auch Drupal ist mit HTML5 kompatibel. Zudem wird das Responsive Webdesign ebenso vollumfänglich unterstützt. Darüber hinaus läuft das System auf allen Browsern, die CSS unterstützen. In dieser Kategorie werden alle Kriterien zur vollsten Zufriedenheit erfüllt.

Unternehmenseinsatz

Plattformunabhängigkeit:

Drupal unterstützt die Webserver Apache, Nginx und Microsoft ISS. Als Datenbanken können MySQL, SQLite und PostgreSQL verwendet werden. Zudem werden die Skriptsprachen PHP und JavaScript unterstützt. Eine große Hürde stellt die nicht allzu gebräuchliche aspektorientierte Entwicklung dar. Zudem ist Drupal ebenfalls nicht zu Oracle-Datenbanken kompatibel. Als Betriebssystem werden Linux, Microsoft Windows und Macintosh OSX unterstützt.

Berechtigung innerhalb des Systems:

Eine automatische Berechtigungszuweisung ist durch eine Schnittstelle zu einem LDAP-Server über eine Erweiterung möglich. Zudem besteht ein die Möglichkeit Benutzerrollen anzulegen und zu verwalten. Allerdings fehlt neben der Mandantenunterstützung auch die Möglichkeit Benutzerberechtigungen zu vererben.

Aufwand:

Die Installation war intuitiv gestaltet. Allerdings trat auch hier während des Installationsprozesses ein Fehler auf. Darüber hinaus müssen zahlreiche Module nachinstalliert werden, da diese in der Core-Version nicht enthalten sind. Updates lassen sich ebenfalls nicht automatisiert durchführen. Diese müssen auch hier manuell von Experten vorgenommen werden.

Templateverwaltung/ -erstellung:

Es ist möglich sowohl von Websites als auch von einzelnen Inhalten Vorlagen zu erstellen und diese zu verwalten.

Open Source

Community:

Mit einer Größe von rund 750.000 Mitgliedern ist die Community von Drupal die größte. Die Summe aller Forenbeiträge beläuft sich auf insgesamt 1,2 Millionen und belegt damit lediglich den zweiten Rang.

Dokumentation:

Bei den Dokumentationen gibt sich Drupal genauso keine Blöße. Neben einer Codedokumentation, einem Benutzer- und Entwicklerhandbuch ist sogar ein FAQ vorhanden. Die Dokumentationen sind wie bei Joomla! derzeit nur auf Englisch vorhanden.

Verbreitungsgrad:

Seit dem Jahr 2008 gibt es leider keine zuverlässigen Erhebungen bzgl. der Downloadanzahl. Die letzte Erhebung im Jahr 2008 ergab rund 1,4 Millionen Downloads. Mit nur 26 Entwicklern belegt Drupal mit großem Abstand den letzten Rang.

Support:

Für das System sind zahlreiche hilfreiche Tutorials vorhanden. Allerdings fehlt ein Wiki für den Selbstsupport. Zudem gibt es auch hier nur sehr eingeschränkten Support durch Dienstleister für dieses System.

Sonstige:

Das System unterstützt derzeit über 80 unterschiedliche Sprachen. Mit rund 710 Tausend Websites die auf Basis von Drupal erstellt wurden, belegt Drupal derzeit im Vergleich zu den anderen Systemen den zweiten Rang. Der Marktanteil im deutschsprachigen Bereich beträgt aktuell 4%. Das System ist mit einem Produktalter von 13 Jahren das zweitälteste System.

7.4.4 Fazit der Untersuchung

Als Ergebnis der durchgeführten Nutzwertanalyse belegt TYPO3 mit einer Score von 79,9 knapp den ersten Rang. Auf Rang zwei landete Joomla! mit einer Score von 76,6. Mit einem Abstand von knapp zehn Punkten belegt Drupal den dritten Rang mit einer Score von 67,5. Aus dem Ergebnis leitet sich generell folgende Empfehlung ab. TYPO3 eignet sich hervorragend für den Einsatz im Unternehmensumfeld. Speziell wegen dem sehr umfangreichen Rechtemanagement welches in diesem System vorhanden ist. Auf Grund der fehlenden Mandantenfähigkeit eignet sich Joomla! eher für Websites bei denen kein umfangreiches Rechtemanagement notwendig sind. Drupal weist ebenfalls für den Einsatz im Unternehmensumfeld zu viele Defizite auf. So eignet sich das System generell für Websites bei denen viel Wert auf Social Publishing gelegt wird.

8 Schlussbetrachtung und Ausblick

Ziel dieser Arbeit war ein Kriterienkatalog zu entwerfen, welcher Unternehmen bei der Wahl eines geeigneten CMS unterstützen soll. Es wurde ein Marktüberblick über vorhandene OS CMS gegeben, aus denen insgesamt drei Systeme ausgewählt wurden, um die Anwendbarkeit des Kriterienkatalogs zu beweisen. Abschließend wurde das Ergebnis jedes einzelnen Systems dargelegt und eine Einsatzempfehlung gegeben.

Unter Anwendung des erstellten Kriterienkataloges kann eine umfangreiche Differenzierung unterschiedlicher CMS erfolgen. Auf Grundlage dessen ist es möglich, eine Auswahl für den Einsatz eines Systems zu treffen. Der Kriterienkatalog wurde in eine Nutzwertanalyse integriert. Dadurch können die Kriterien dynamisch ausgewählt, gewichtet und betrachtet werden. Zudem wurden zur komfortableren Verwendung diverse Masken erstellt, über die der Anwender zu Beginn die Gewichtung der Ober- und Unterkategorien sowie der einzelnen Kriterien festlegen kann. Im Folgeschritt kann die Bewertung dieser vorgenommen werden. Zudem besteht die Möglichkeit gewisse Vorgaben oder Kommentare anzugeben.

In Zukunft bietet es sich an vor allem Folgearbeiten im Bereich der Eingabemasken vorzunehmen, um den Eingabekomfort weiter steigern zu können. Es bietet sich vor allem an, die Masken dynamisch aufzubauen und je nach Auswahl weitere Inhalte anzuzeigen. Zudem sind Plausibilitätsprüfungen notwendig um Fehleingaben abfangen zu können und somit die Robustheit des Kriterienkatalogs weiter zu steigern. Darüber hinaus kann es neben den knapp 100 Kriterien weitere spezielle Anforderungen von Seiten eines Unternehmens geben. Solche speziellen Anforderungen und Sonderfälle wurden in Rahmen dieser Arbeit nicht betrachtet. Daher wird es zukünftig notwendig sein, weitere Kriterien für solche Einzelfälle in den Kriterienkatalog aufzunehmen.

Mit der durchgeführten Marktanalyse der bestehenden OS CMS wird ein Überblick über die unterschiedlichsten Systeme gegeben. Um diese auf deren potentielle Eignung hin zu überprüfen wurden Auswahlkriterien festgelegt, anhand derer eine Eingrenzung erfolgte. Dadurch wurden drei Systeme identifiziert, die exemplarisch näher untersucht werden sollten.

Die abschließende exemplarische Untersuchung der zuvor festgelegten drei CMS belegt die Anwendbarkeit des Kriterienkataloges. Hierfür wurden exemplarisch ausgewählte Unterkategorien betrachtet und anhand von den jeweiligen Ausprägungen der Systeme bewertet. Das daraus resultierende Ergebnis wurde abschließend zusammengefasst und eine Einsatzempfehlung für die Systeme abgegeben. Damit wurde bewiesen, dass für Unternehmen eine differenzierte Betrachtung verschiedener CMS, über den erarbeiteten Kriterienkatalog und die aufgebaute Nutzwertanalyse, ermöglicht wird. Jedes Unternehmen kann auf Grundlage dessen selbst entscheiden welches OS CMS die gestellten Anforderungen am besten erfüllt.

Anhang

Anhangverzeichnis

Anhang 1: Eingabemaske zur Gewichtung der Kriterien

Gewichtung der Kriterien

CMS allgemein | Unternehmenseinsatz | Open Source |

Bitte verteilen Sie die Gewichtung für jedes Kriterium. Für jedes einzelne Kriterium sind 100% zu vergeben

CMS allgemein

Technische Spezifikation

Skalierbarkeit: 0

Wechselbarkeit der Datenbank: 0

Visualisierung: 0

Clusterbetrieb: 0

Erweiterbarkeit

durch Plugins: 0

durch Module: 0

Integration von Anwendungen: 0

Suchmaschinenfreundlichkeit

Sprechende URLs möglich: 0

Erstellen einer Sitemap: 0

Metadatenhinterlegung zu Websites: 0

Funktionalitäten

Existierendes Versionsmanagement: 0

Backup und Widerherstellungsmöglichkeit: 0

Offlinearbeit über lokale Kopie: 0

Suchfunktion vorhanden: 0

Erweiterte Funktionalitäten vorhanden: 0

PDF-Export mit Aufbereitung: 0

Import/Export von Content zu anderen CMS: 0

Benutzbarkeit

Softwareergonomie: 0

Robustheit: 0

Barrierefreiheit: 0

Besucher: 0

Entwickler: 0

Direkte Navigation auf Websites: 0

Tastatursho rtcuts: 0

Modularer Aufbau und Gestaltung: 0

Personalisierbarkeit der Anwendungsoberfläche: 0

Kompatibilität

Kompatibilität mit HTML5: 0

Unterstützung responsive Webdesign: 0

Browserunabhängig: 0

Editor

Erwartungskonformität: 0

Drag & Drop: 0

Einfache Editierung einer Website: 0

Zwischenspeicherungs-/Widerherstellungsfunktion: 0

Rechtschreibprüfung: 0

Integration von Anwendungen: 0

Gestaltungsfreiraum für Content: 0

Automatische Fehlererkennung in HTML: 0

Medienverwaltung

Medien einbindbar: 0

Mediendownload: 0

Integrierte Bildbearbeitung: 0

Mediengalerie vorhanden: 0

Unterstützung von Kartendienste: 0

Sonstige

Trennung von Inhalt, Darstellung und Metadaten: 0

Aufwärtskompatibilität: 0

Schulungsangebot: 0

Erstellung eines eigenen Blogs: 0

A_Z Indexseite: 0

OK | Zurück | Abbrechen

Anhang 2: Auszug des Quellcodes der Eingabemasken

Jede Eingabemaske besteht aus einem Eingabebereich sowie aus den drei Buttons OK, Zurück und Abbrechen. Die Logik der Buttons soll nachfolgend anhand des Quellcodes erklärt werden.

OK-Button

```
Private Sub cmdOK_Click()
      Range("F7") = FormatPercent(FormatNumber(txtTechnisch) / 100)
      ...
      Unload Me
      ufKriterien.Show
End Sub
```

Der OK-Button besteht generell aus drei unterschiedlichen Befehlen. Zunächst wird auf das Click-Event des Buttons abgefragt. Sobald dieser Geklickt wurde, wird der anschließende Quellcode ausgeführt. Mit dem Befehl „Range("F7")" wird eine bestimmte Zelle der Excel-Tabelle ausgewählt, in diesem Fall wäre das nun die Zelle F7. Dieser Zelle wird nun der Wert der Textbox „txtTechnisch" zugewiesen. Um anschließend den Score korrekt berechnen zu können, wird der Wert allerdings als Prozent formatiert. Der Befehl „Unload Me" bewirkt anschließend, dass die aktuell angezeigte Eingabemaske geschlossen wird. Im Anschluss daran wird durch den Befehl „ufKriterien.Show" die Eingabemaske für die Gewichtung der einzelnen Kriterien angezeigt.

Zurück-Button

```
Private Sub cmdBack_Click()
      Unload Me
      ufKategorien.Show
End Sub
```

Hierbei wird ebenfalls auf das Click-Event des Buttons abgefragt. Sobald der Button geklickt wird, wird der Code ausgeführt. Der Befehl „Unload Me" bewirkt hierbei, dass die aktuell angezeigte Eingabemaske geschlossen wird. Durch den Befehl „ufKategorien.Show" wird anschließend Eingabemaske für die Gewichtung der Kategorien angezeigt.

Abbrechen-Button

```
Private Sub cmdAbbrechen_Click()
      Unload Me
End Sub
```

Hierbei wird genauso auf das Click-Event des Buttons abgefragt. Sobald der Button geklickt wird, wird der Code ausgeführt. Der Befehl „Unload Me“ bewirkt hierbei, dass die aktuell angezeigte Eingabemaske geschlossen wird.

Anhang 3: Marktanalyse OS CMS

1	Alfresco	38	fullxml	75	phpNuke
2	Aman Redsys	39	GetSimple CMS	76	phpwcms
3	artmedic cms-light	40	glonz.com	77	phpWebEd
4	AxCMS	41	gpEasy CMS	78	phpWebSite
5	binarycloud	42	gupsi	79	Pivot
6	bitflux	43	holacms	80	Plone
7	BlackCat	44	Icy Phoenix	81	postNuke
8	blosxom	45	ImpressCMS	82	QuickApps CMS
9	Brainstorm	46	ImpressPages	83	razorCMS
10	calladium	47	Jahia	84	Red Hat Enterprise CMS
11	callistocms	48	Joomla	85	REDAXO
12	CCM	49	Joostina	86	Redaxscript
13	CitrusCMS	50	Kajona	87	Sally-CMS
14	CMBasic	51	Kryn.cms	88	Scientific CMS
15	CMS.R.	52	LEPTON CMS	89	Sefrengo
16	CMSimple	53	LOCOMOTIVECMS	90	SilverStripe
17	Cocoon / Lenya	54	Magnolia	91	Slashcode
18	Concrete5	55	Mambo	92	sNews
19	Contao	56	Mason	93	strg-c
20	contelligent	57	metadot	94	synType CMS
21	CONTENIDO	58	MidGard	95	Textpattern
22	ContentLion	59	mmbase	96	Tiki Wiki CMS
23	Contrexx	60	MODX	97	Tribiq
24	corinis	61	moveabletype	98	TYPO3
25	Der Dirigent	62	Moxeo	99	Umbraco
26	django CMS	63	Newscoop	100	uPortal
27	DotNetNuke	64	Nucleus CMS	101	web@all CMS
28	Drupal	65	NukeViet	102	Webgui
29	e107	66	Odls	103	WebInsta
30	EasyHP	67	OneCMS	104	WebsiteBaker
31	Elxis	68	OpenCMS	105	Wolf CMS
32	eoCMS	69	open-medium.cms	106	Wordpress
33	Etomite	70	PAPAYA	107	xinity
34	eZ publish	71	Papoo	108	Xoops
35	FarCry	72	Papp	109	xSiteable
36	Fork	73	phpCMS	110	Zikula
37	Frog	74	PHP-Fusion	111	ZMS

Anhang 4: Detailliertere Analyse der existierenden OS CMS

CMS		Anzahl der Entwickler[57]	Produkt-alter	Veröffentlichungs-häufigkeit (Stand 23.12.2013–12:00 Uhr)	Rollen-konzept
1	Plone	222	2004	3 Tage	ja[58]
2	Joomla!	221	2005	2 Tage	ja[59]
3	TYPO3	155	1998	22 Tage	ja[60]
4	SilverStripe	146	2000[61]	2 Tage	ja[62]
5	Umbraco	92	2003[63]	3 Tage	ja[64]
6	django CMS	83	2007[65]	3 Tage	nein
7	eZ publish	70	1999	3 Tage	ja
8	Concrete5	54	2003	9 Tage	ja[66]
9	Tiki Wiki CMS	50	-	10 Stunden	ja[67]
10	LOCOMOTIVECMS	36	-	13 Tage	nein
11	Alfresco	35	2005[68]	4 Tage	ja[69]
12	MODX	35	-	3 Monate	nein
13	Magnolia	33	-	3 Tage	ja[70]
14	Contao	31	-	3 Tage	ja[71]
15	Drupal	26	2001	14 Stunden	ja[72]
16	Zikula	22	-	3 Tage	**ja**[73]
17	Wordpress	20	-	1 Tag	ja[74]
18	Jahia	18	-	3 Tage	ja[75]
19	PAPAYA	17	-	4 Tage	ja[76]

57 Vgl. ohloh (2014)
58 Vgl. Concrete5 (o.J.)
59 Vgl. Ebersbach, A./Glaser, M./Kubani, R. (2009), S 184 f.
60 Vgl. HTMLWorld
61 Vgl. SilverStripe (o. J.a)
62 Vgl. SilverStripe (o. J.b)
63 Vgl. Umbraco (o. J.)
64 Vgl. Contentmanager.de (2013b)
65 Vgl. CMS Garden (o. J.)
66 Vgl. Concrete5 (2014)
67 Vgl. Tikiwiki CMS Groupware (2014)
68 Vgl. Alfresco (2014a)
69 Vgl. Alfresco (2014b)
70 Vgl. Magnolia Dokumentation (2013)
71 Vgl. Visual4 (o. J.a)
72 Vgl. ebenda
73 Vgl. Zikula Community (o. J.)
74 Vgl. Visual4 (o. J.b)
75 Vgl. Jahia (o. J.)

20	DotNetNuke	16	-	3 Monate	ja[77]
21	OpenCMS	15	-	3 Monate	ja[78]
22	Newscoop	14	-	12 Tage	ja[79]
23	FarCry	13	-	22 Stunden	ja[80]
24	Wolf CMS	13	-	1 Monat	ja[81]
25	gpEasy CMS	11	-	6 Monate	-
26	ImpressCMS	10	-	30 Tage	-
27	ImpressPages	10	-	Ca. 2 Monate	-
28	CMSimple	7	-	Vor 3 Tage	-
29	Jaws	7	-	3 Tage	-
30	Kajona	6	-	2 Tage	-
31	REDAXO	6	-	1 Monat	-
32	e107	5	-	7 Monate	
33	Icy Phoenix	5	-	1 Monat	
34	LEPTON CMS	5	-	14 Tage	
35	Sally-CMS	5	-	6 Tage	
36	BlackCat	3	-	3 Tage	
37	calladium	-	-	Herbst 2013	
38	CMBasic	-	-	Ca. 6 Monate	
39	contelligent	-	-	Ca. 4 Monate	
40	ContentLion	-	-	Ca. 2 Monate	
41	Contrexx	-	-	Ca. 1 Monat	
42	moveabletype	-	-	Ca. 2 Monate	
43	Sefrengo	-	-	Ca. 1 Monat	

[76] Vgl. Papaya (o. J.)
[77] Vgl. DNN Creative.com (2014)
[78] Vgl. OpenCMS (2010)
[79] Vgl. Flossmanuals.net (o. J.)
[80] Vgl. Confluence (2010)
[81] Vgl. WolfCMS (2011)

Quellenverzeichnisse

Literaturverzeichnis

Abts, D./Mülder, W. (2011): Grundkurs Wirtschaftsinformatik, Eine kompakte und praxisorientierte Einführung, 7. Aufl., Wiesbaden: Vieweg+Teubner Verlag

Abts, D./Mülder, W. (2010): Masterkurs Wirtschaftsinformatik, Kompakt , praxisnah, verständlich- 12 Lern- und Arbeitsmodule, 1. Aufl., Wiesbaden: Vieweg+Teubner Verlag

Becker-Pechau, P./ Roock, S./Sauer, J. (2004): Open Source für die Software-Entwicklung, in: Open-Source-Software, Heidelberg: dpunkt.verlag

Bodendorf, F. (2006): Daten- und Wissensmanagement, 2. Aufl., Heidelberg: Springer-Verlag

Ebersbach, A./ Glaser, M./Kubani, R. (2009): Joomla! 1.5, , 2. Aufl., Bonn: Galileo Press

Fröschle, H-P./Reich, S. (2007): Enterprise Content Management, Heidelberg: dpunkt.verlag GmbH

Gersdorf, R. (2003): Content Management für die flexible Informationswiederverwendung, in: Content Management Handbuch, Strategien, Theorien und Systeme für erfolgreiches Content Management, St. Gallen: NetAcademy Press Verlag

Graf, H. (2008): Drupal 6: Websites entwickeln und verwalten mit dem Open Source-CMS, München: Addison-Wesley Verlag

Hinkelmann, K./Urech, R. (2010): ECM Enterprise Content Management, Plan, Build, Run-vom Bedarf zur Realisierung, Rheinfelden/Schweiz: Best Practice Xperts

Kempkens, A., (2009): Das Joomla! Entwicklerhandbuch, Joomla!-Komponenten und Templates programmieren mit dem Joomla!-Framework, München: Addison-Wesley Verlag

Luhm, T. (2011): Das Einsteigerseminar Drupal 7, Heidelberg/München/Landsberg/Frechen/Hamburg: Verlagsgruppe Hühtig Jehle Rehm GmbH

Manhart, K./Zimmermann, M. (o. J): Basiswissen SOA, BI, CRM, ECM, Grundlagen , Methoden, Praxis, München: IDG Business Media GmbH

Meyer, R.(2013): Praxiswissen TYPO3, 6. Aufl., Köln: O`Reilly Verlag

Nix, M. et al. (2005): Web Content Management, CMS verstehen und auswählen, Frankfurt: Software & Support Verlag GmbH

Schwarzer, B./Krcmar, H. (2010): Grundlagen betrieblicher Informationssysteme, 4. Aufl., Stuttgart: Schäffer-Poeschel Verlag

Stahl, F. /Maass, W. (2003): Glossar zu Fachbegriffen aus dem Umfeld von Content Management Fachbegriffen, in: Content Management Handbuch, Strategien, Theorien und Systeme für erfolgreiches Content Management, St. Gallen: NetAcademy Press Verlag

Stahl, F./Schettler, O. (2012): Praxiswissen Drupal 7, 2. Aufl., Köln: O`Reilly Verlag GmbH & Co.KG

Riggert, W. (2009): ECM-Enterprise Content Management, Konzepte und Techniken rund um Dokumente, 1. Aufl., Wiesbaden: Vieweg+Teubner Verlag

Zschau, O. (2003): Web CMSe – Eine kurze Einführung, in: Content Management Handbuch, Strategien, Theorien und Systeme für erfolgreiches Content Management, St. Gallen: NetAcademy Press Verlag

Verzeichnis der Internet- und Intranet-Quellen

Alfresco (2014a): Unsere Kunden leisten großartige Arbeit, https://www.alfresco.com/de/alfresco-ebook-zu-kundenprojekten, Abruf 03.01.2014

Alfresco (2014b): Benutzerrollen und Berechtigungen, http://www.alfresco.com/help/webclient/concepts/cuh-user-roles-permissions.html, Abruf 03.01.2014

CMS Garden (o. J.): django CMS, http://www.cms-garden.org/de/cms/django-cms, Abruf: 25.12.2013

Concrete5 (o. J.): History, http://www.concrete5.org/about/our_philosophy/history/, Abruf: 03.01.2014

Concrete5 (2014): Working with Permissions, https://www.concrete5.org/documentation/introduction/switch-and-learn/custom-content-in-wordpress-and-concrete5/working-with-permissions-in-wordpress-and-concrete5/, Abruf: 03.01.2014

Confluence (2010): Benutzer, Gruppen, Rollen und Berechtigungen, https://farcry.jira.com/wiki/pages/viewpage.action?pageId=12943480, Abruf: 03.01.2014

Contentmanager.de (2013a): Spezielle Anforderungen an CMSe für den Mittelstand, http://www.contentmanager.de/magazin/spezielle_anforderungen_an_content_management_systeme_fuer.html, Abruf: 11.12.2013

Contentmanager.de (2013b): Phone im Überblick – Teil 2, Das Open-Source-cms AUF Pytho Basis im Detail, http://www.contentmanager.de/magazin/plone_cms_fuer_anspruchsvolle_anwender-2.html#benutzer_und_rechteverwaltung, Abruf: 23.12.2013

Diehl, A. (o. J.): TYPO3 und Wordpress im Vergleich, http://www.estrategy-magazin.de/typo3-wordpress-vergleich.html, Abruf: 16.01.2014

DNN Creative.com (2014): DotNetNuke Modul Seite und Berechtigungen, http://www.dnncreative.com/Tutorials/DNNTutorialsforAdministra-tors/ModuleandPagePermissions/tabid/531/Default.aspx, Abruf: 03.01.2014

Flossmanuals.net (o. J.): Benutzerverwaltung, http://en.flossmanuals.net/newscoop-4-journalists-en-4-0/user-management/, Abruf: 03. 01.2014

Gabler Wirtschaftslexikon (o. J.): Open Source, http://wirtschaftslexikon.gabler.de/Archiv/77360/open-source-v7.html, Abruf: 31.12.2013

Google (2014): Interesse im zeitlichen Verlauf, http://www.google.de/trends/explore#q=joomla%2C%20typo3%2C%20silverstripe&cmpt=q, Abruf 13.01.2014

HTMLWorld (o. J.): Typo3: Benutzer und Benutzergruppen, http://www.html-world.de/program/typo3_9.php, Abruf: 25.12.2013

Jahia (o. J.): Authorization Systemkonzepte, http://www.jahia.com/community/documentation/roles/concepts.html, Abruf: 02.01.2014

Joomla! (o. J.): Was ist Joomla!, http://www.joomla.de/joomla-entdecken, Abruf: 14.01.2014

Ksi Consulting (2012): Verbreitung der CMS-Systeme im Vergleich – Drupal, Joomla!, TYPO3, WordPress, http://www.ksi-cms.de/content/verbreitung-cms-systeme-drupal-joomla-typo3-wordpress, Abruf: 16.01.2014

Magnolia Dokumentation (2013): Default Permissions, http://documentation.magnolia-cms.com/display/DOCS/Default+permissions, Abruf: 26.12.2013

Ohloh (2014): Disover, Track and Compare Open Source, http://www.ohloh.net/, Abruf: 23.12.2013

OpenCMS (2010): Wie OpenCMS Berechtigungen arbeiten, http://www.opencms-wiki.org/wiki/How_OpenCms_Permissions_work, Abruf: 28.12.2013

Papaya (o. J.): FAQ Bedienung & Administration, http://www.papaya-cms.com/faq.998.de.html?ff: faqgroup_id=1, Abruf 03.01.2014

SilverStripe (o. J.a): Unsere Geschichte, http://www.silverstripe.org/our-history/, Abruf: 25.12.2013

SilverStripe (o. J.b): Verwalten von Rollen und Berechtigungen, http://userhelp.silverstripe.org/framework/en/for-website-administrators/managing-roles-and-permissions, Abruf: 25.12.2013

Tikiwiki CMS Groupware (2014): Permissions Settings, https://doc.tiki.org/ Permis-sions, Abruf 02.01.2014

TYPO3 (o. J.a): The History of TYPO3, http://typo3.org/about/typo3-the-cms/the-history-of-typo3/, Abruf: 12.01.2014

TYPO3 (o. J.b): About the name, http://typo3.org/the-brand/about-the-name/, Abruf: 12.01.2014

TYPO3 (o. J.c): TYPO3 CMS-The Enterprise CMS, http://typo3.org/about/typo3-cms/, Abruf: 12.01.2014

Umbraco (o. J.): Geschichte, http://umbraco.com/about-us/history .aspx, Abruf: 25.12.2013

VFSI (2012): WordPress, Drupal oder Joomla!? Welches CMS ist das „richtige“?, http://www.vfsi.at/wordpress-drupal-oder-joomla-welches-cms-ist-das-richtige/, Abruf: 14.01.2014

Visual4 (o. J.a): CMS-Vergleich Open Source CMS-Systeme im Vergleich, http://www.visual4.de/open-source-cms-system/cms-vergleich-joomla-wordpress-typo3-drupal-contao-plone.html, Abruf 28.12.2013

Visual4 (o. J.b): CMS-Vergleich Open Source CMS-Systeme im Vergleich, http://www.visual4.de/open-source-cms-system/cms-vergleich-joomla-wordpress-typo3-drupal-contao-plone.html, Abruf 28.12.2013

W3Techs (2014): Marktanteil jährlich Trends für CMSe für Websites, http://w3techs.com/technologies/history_overview/content_management/ms/y, Abruf: 14.01.2014

Webkalkulator (o. J.a): CMS-Vergleich: WordPress vor Joomla! und typo3, http://www.webkalkulator.com/w_content/nr_blog/artikel_2011/M01/cms-websites.asp?id=11, Abruf: 12.01.2014

Webkalkulator (o. J.b): CMS Marktanteile & CMS Budgets, http://www.webkalkulator.com/cmsvergleich, Abruf: 13.01.2014

WolfCMS (2011): Einführung, http://www.wolfcms.org/wiki/plugins:roles_and_permissions, Abruf: 03.01.2014

WordPress (o. J.): Support: Getting Started, http://en.support.wordpress.com/getting-started/, Abruf: 16.01.2014

Zikula Community (o. J.): Programmierung von Berechtigungen in Zikula, http://community.zikula.org/index.php?module=Wiki&tag=ZikulaPermissions, Abruf: 26.12.2013

Duale Hochschule
Baden-Württemberg
Stuttgart

Open Source Security Checktoolsfür Penetration Tests

Am Beispiel von Portscannern

Schriftliche Ausarbeitung
im Rahmen der Lehrveranstaltung „Forschungsprojekt KOS“

Vorgelegt von

Heike Binner,
Dominique Gallus,
Alexandra Höger,
NeedaMontazeri

am 31.01.2014

Fakultät Wirtschaft
Studiengang Wirtschaftsinformatik
WWI2011V

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACK	Acknowledgement
BDSG	Bundesdatenschutzgesetz
DHBW	Duale Hochschule Baden-Württemberg
FIN	Finish
GoB	Ordnungsgemäße Buchführung
GoBs	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GUI	Graphical User Interface
HGB	Handelsgesetzbuch
ICMP	Internet-Protokoll-Message-Protocol
IKS	Interne Kontrollsysteme
IP	Internet Protocol
IPID	IP Identification-Number
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
Nast	Network Analizer Sniffer Tool
NMap	Network Mapper
Penetrationtest	Pen-Test
RPC	Remote Procedure Call
RST	Reset
SYN	Synchronize
TCP	Transmition Control Protocol
UDP	User Datagramm Protocol
ZKDSG	Zugangskontrolldienstschutzgesetz

Abbildungsverzeichnis

Tabellenverzeichnis

1Einleitung

Die Internetseite „sicherheitstacho.eu“ zeigt Angriffe in realer Zeit. Die Daten werden dabei von 97 Honeypot-Systemen gesammelt. Diese simulieren eine ungesicherte Umgebung und sollen so die Hacker zu einem Angriff verleiten[1]. Laut Sicherheitstacho.de versuchten allein im letzten Monat (30/12/13) 1.686.390 Personen aus den Niederlande, 878.002 aus der USA und 421.791 aus Deutschland das System zu hacken[2]. Dies zeigt, dass Rechner im privaten Gebrauch, sowie in Unternehmen vor Angriffen geschützt werden müssen. Für Firmen ist der Schutz von Informationenrechtlich vorgeschrieben.

Um die Sicherheit von Daten gewährleisten zu können, werden neben Firewallsystemen und Anti-Viren Programmen zudem auch Penetration Tests durchgeführt. Mit diesen Tests können Schwachstellen eines Systems aufgedeckt werden. Dabei wird zwischen organisatorischen und technischen Penetration Tests unterschieden. Die Arbeit beschränkt sich auf den technischen Bereich, d.h. dass kontrollierte, gezielte Angriffe auf ein System oder eine bestimmte Software ausgeführt werden. In dieser Ausarbeitung werden nur Port Scanner beleuchtet. Diese Tools können eine Vorbereitung für den eigentlichen Angriff eines Hackers bilden, wenn damit beispielsweise offene Zugangspunkte, Ports, des Systems damit aufgelistet werden.

Zu Beginn werden die Grundlagen zu den Penetrationstest sowie Security Check Tools erläutert. Auf dieser Basis wird detaillierter auf die Portscanner eingegangen und ausgewählte Tools vorgestellt. Diese wurden im Laufe des Projekts getestet. Mit Hilfe der Ergebnisse aus den Tests und den aufbereiteten Informationen wurde ein Kriterienkatalog erstellt. Dieser dient als Grundlage, ein passendes Werkzeug für die Durchführung eines Scans zu finden. Zum Abschluss werden mit Hilfe von verschiedenen Auswahlkriterien z.B. technische Affinität des Anwenders, welche sich je nach Anforderungen unterscheiden mehrere Entscheidungsmöglichkeiten aufgezeigt und erläutert.

[1] Wendehost T. (2013)
[2] o. V. (2014 a)

2Penetrationstests

2.1 Definition

Bei Penetrationstests werden kontrollierte Angriffe auf ein IT-System simuliert um damit die Sicherheit des Computernetzwerkes beziehungsweise -systems zu überprüfen. Das Ziel ist die Aufdeckung und Identifikation von potenziellen Systemsicherheitslücken oder Schwachstellen innerhalb eines Netzwerkes. Durch jene Ermittlung der Sicherheitsmängel kann schließlich der Schutz des technischen Systems, sowie von organisatorischen Infrastrukturen verbessert werden. Penetrationstests dienen zudem als Gewährleistung des Sicherheitsniveaus innerhalb einer Zertifizierung oder gegenüber Dritten wie zum Beispiel Kunden.

Penetrationstests (Pen-Tests) können in zwei Typen klassifiziert werden. Zum einen als klassischer Pen-Test, bei welchem ein Angriff auf ein vollständiges Firmennetzwerk oder auf dessen einzelnen Bestandteile durchgeführt wird. Der zweite Vorgehenstyp beinhalten die Produktpenetrationstests. Hier wird ein Produkt, welches sicherheitstechnisch besonders zu berücksichtigen ist, auf eventuelle Schwachstellen und Sicherheitslücken überprüft. Ebenso wird zwischen internen und externen Pen-Tests unterschieden. Wobei die externen Tests über öffentliche Netze, wie zum Beispiel das Internet, durchgeführt werden. Interne Tests erfolgen hingegen über einen bereits vorhandenen Zugriff auf das betroffene Netzwerk oder System.[3]

2.2 Security Check Tools

Um Penetrationstests durchzuführen, werden sogenannte „Security Check Tools“ eingesetzt. Diese Tools finden und dokumentieren Sicherheitslücken. Dazu simulieren sie während des Penetrationstests unterschiedliche Angriffe auf ein Netzwerk, eine Anwendung oder Ähnliches. Durch die Nutzung werden vorhandene Schwachstellen und Angriffsmöglichkeiten ermittelt um das Risiko eines unberechtigten Zugriffs zu minimieren.[4]

Es gibt verschiedene Werkzeuge, unter anderem Passwortcracker oder Portscanner. Je nach gewünschtem Ziel, kann zwischen den verschiedenen Tools, die dafür geeignet sind, gewählt werden[5].

[3] Vgl. Freiling F./Liebchen J., S. 1 f.
[4]Vgl. BSI (2003), S. 8
[5]Vgl. ebenda, S. 133 ff.

So gibt es beispielsweise bei Portscannern die Auswahl zwischen ca. 15 Tools, welche sich sowohl im Umfang als auch bei der Vorgehensweise unterscheiden. Angriffe auf ein Netzwerk können z.B. versteckt oder offen durchgeführt werden[6].Durch unterschiedliche Anforderungen an die Security Software, müssen verschiedenen Zielsetzungen im Vorfeld definiert werden. Hierbei sollten die IT-Sicherheit, sowie der Fachbereich miteinbezogen werden. Zu beachten ist dabei, welche Angriffsform für den Penetrationstest geeignet ist. Dabei ist auch auf gesetzliche Vorgaben zu achten, welche im folgenden Kapitel beschrieben werden.

2.3Rechtliche Grundlagen

2.3.1 Gesetztestexte

Ein Unternehmen ist gesetzlich nicht dazu verpflichtet Penetrationstests durchzuführen[7]. Es ist jedoch für die Sicherheit, sowie die Verfügbarkeit, Vertraulichkeit und Integrität seiner Daten verantwortlich. Maßnahmen um dies zu gewährleisten sind unter anderem Firewallsysteme und darüber hinaus ausgearbeitete Sicherheitskonzepte. Eine Integration solcher Systeme reicht jedoch nicht immer aus, um die gesetzlichen Vorgaben zu 100 Prozent zu erfüllen. Aus diesem Grund werden Penetrationstests durchgeführt, um so die Funktionalität der vorgenommenen Maßnahmen zu prüfen.

Verschiedene Gesetzestexte beschreiben die gesetzliche Regelung dieser Sicherheitsmaßnahmen. Dabei handelt es sich unter anderem um das Handelsgesetzbuch (HGB), das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) oder die Grundsätze ordnungsmäßiger Datenverarbeitung-gestützter Buchführungssysteme (GoBS).

Das HGB legt die Richtlinien zur ordnungsgemäßen Buchführung (GoB) bzw. die GoBS fest. Im letzteren werden die Regeln für die Buchführung, welche mit Hilfe eines Datenverarbeitungssystems durchgeführt werden, beschrieben.[8] Der vierte Abschnitt der GoBS beschreibt die Vorschriften für ein Internes Kontrollsystem (IKS). Bei diesen handelt es sich um alle Kontrollen, Maßnahmen und Regelungen zum Schutz der vorhandenen Informationen. Der fünfte Abschnitt enthält alle Bestimmungen zur Datensicherheit.

Die Sicherheitsbedingungen für die Arbeit mit personenbezogenen Daten sind im Bundesdatenschutzgesetz festgelegt. In diesem werden die organisatorischen und technischen Maßnahmen geschildert.

---

[6] Vgl. ebenda, S. 12 f.
[7] Vgl. Kendinibilir B. (2010)
[8] Vgl. BSI (2003), S. 18 f.

Ein Ausschnitt aus dem Gesetzestext macht dies deutlich. „Öffentliche und nichtöffentliche Stellen, die [...] personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes [...] zu gewährleisten.“ (§ 9 BDSG).

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist im Mai 1998 in Kraft getreten. Es regelt die Berichtspflicht von Aktiengesellschaften gegenüber dem Aufsichtsrat[9]. Dieser Bericht handelt über das Risikomanagement, welches im Gesetz nicht exakt ausformuliert ist. Es sind jedoch Pflichten für sogenanntes Frühwarnsysteme oder Überwachungssysteme beschrieben.

EU-weit gibt es zudem Datenschutzrichtlinien, welche 1995 erlassen wurde[10]. Darin wird auf die Notwendigkeit von Sicherheitskonzepten im Unternehmen hingewiesen. Der Gesetzestext sagt aus, dass technische und organisatorische Maßnahmen getroffen werden müssen, um sich gegen zufällige und unrechtmäßige Zerstörung von personenbezogenen Daten zu schützen. Ebenso vor zufälligen Verlusten, eine unberechtigte Veränderung, die unberechtigte Weitergabe, den unberechtigten Zugang oder jeder andere Form von unrechtmäßiger Verarbeitung. Dieser Schutz gilt insbesondere für Daten, die über ein Netzwerk übertragen werden.

Neben diesen beschriebenen Gesetztestexten gibt es noch den Staatsvertrag für Mediendienste (MDStV), das Teledienstgesetz (TDG) und Teledienstdatenschutzgesetz (TDDSG), die Telekommunikationsgesetz (TKG), strafrechtliche Vorschriften, das Betriebsverfassungsgesetz (BetrVG) und das europäische Cybercrime-Konvention[11]. Alle diese Niederschriften und Gesetze beschreiben die Verpflichtungen des Unternehmens für den Schutz verschiedenster Daten.

2.3.2 Rechtliche Grundlagen bei der Durchführung

Wird ein Penetrationstest durchgeführt, kann es sein, dass ein Tester Handlungen ausführt, durch die er sich ohne die Einwilligung des Auftraggebers strafbar macht. Aus diesem Grund gibt es strafrechtliche Vorschriften. In diesen werden die Inhalte und der Umfang von Penetrationstests festgelegt. Damit schützt sich der Tester vor rechtlichen Folgen. Es ist essenziell, dass die Rahmenbedingungen genau beschrieben sind. Darüber hinaus gibt es weitere Vorschriften, welche die Einwilligung des Auftraggebers benötigen.

---

[9] Vgl. Wagner F. (o.J.)
[10] Vgl. o.V. (o.J.a)
[11] Vgl. BSI (2003), S. 26 f.

Diese sind im Zugangskontrolldienstschutzgesetz (ZKDSG) niedergeschrieben. Bei einem Zugangskontrolldienst handelt es sich in der Regel um ein technisches Verfahren. Dieses ermöglicht die Verwendung eines zugangskontrollierten Dienstes. Mit diesem Gesetz schützt der Gesetzgeber kostenpflichtigen Diensten wie beispielsweise PayTV vor dem nicht rechtmäßigen Umgehen der Sicherheitsmechanismen[12].

Ein Beispiel für einen solchen Dienst ist ein passwortgeschützter World Wide Web-Server. Führt der Tester einen Penetrationstest durch, versucht er mittels Software das Passwort zu umgehen und auf den Server zuzugreifen. Dabei verstößt er automatisch gegen das ZKDSG. Aus diesem Grund wird im § 3 (ZKDSG) Absatz 1 die Herstellung, Einfuhr und Verbreitung, in Absatz 2 der Besitz, die technische Einrichtung, Wartung und der Austausch und in Absatz 3 die Absatzförderung dieser Umgehungsvorrichtungen für gewerbsmäßige Zwecke erlaubt[13]. Der Tester muss sich trotzdem immer ordnungsgemäß verhalten. Sollte er das nicht tun kann er mit einer Geldstrafe von bis zu 50.000 € belangt werden.

Im Vorhinein werden aus diesem Grund Verträge zwischen Auftraggeber und Auftragnehmer geschlossen in denen die Rechte und Pflichten von beiden Parteien schriftlich festgehalten sind.

2.3.3 Vertragsvereinbarungen bei Penetrationstests

Diese Verträge müssen immer von beiden Parteien akzeptiert werden. So kann in einem möglichen Gerichtsverfahren auf dieses Dokument zugegriffen werden. Ein Penetrationstest ist in der Regel aus Vertragssicht eine entgeltliche Geschäftsbesorgung mit Dienstleistungscharakter. Dabei schuldet der Auftragnehmer dem Auftraggeber lediglich die Leistung jedoch kein Erfolg.

Ein Vertragsgegenstand ist zum Beispiel der Umfang und Inhalt der eingesetzten Mittel, die Zielsetzung oder Art des Penetrationstest. Gängige Zielsetzungen sind beispielsweise:

- Höhere Sicherheit der technischen Systeme
- Aufdeckung von Schwachstellen
- Zertifizierung durch Dritte[14]

[12] Vgl. BSI (2003), S. 28 f.
[13] Vgl. o.V. (2014 b)
[14] Vgl. BSI (2003), S. 31 f.

Im Vertrag werden zudem bestimmte Klassifizierungsmerkmale beschrieben. An Hand dieser wird dann die Penetrationstestart festgelegt. Mögliche Merkmale können sein

- Verdeckte oder offene Vorgehensweise
- Passives Scannen oder aggressives Vorgehen
- Begrenzter, fokussierter oder unbegrenzter Umfang

Unter Berücksichtigung dieser Punkte wird der Vertrag für die Durchführung des Penetrationstest individuell gestaltet. Aus diesem Schriftstück ergeben sich aber nicht nur Rechte.

So hat der Auftraggeber möglicherweise die Aufgabe die für den Test benötigten Informationen dem Tester zur Verfügung zu stellen. Zudem muss er Dritte, die eventuell betroffen sind informieren, „da bei normalem Datenverkehr über öffentliche Netze auch Systeme von (z.B. Webserver eines Hosters) genutzt werden.“ Er kann ebenfalls die Plicht haben, Schutzmaßnahmen für mögliche Systemausfälle vorzunehmen. Dies ist vor allem im Sinne des Auftraggebers, da er angehalten ist, für betroffene Daten und Systeme eine Sicherheitskopie anzufertigen. Ein durch den Penetrationstest ausgelösten Systemausfall führt so zu keinem Datenverlust.

Der Auftragnehmer hat möglicherweise die Pflicht der Verschwiegenheit und die allgemeine Sorgfaltspflicht. Das heißt dass er auf keinen Fall grob fahrlässig handeln darf. Ein Beispiel wäre das Durchführen eines Penetrationstest welcher zu Schäden an Dritten führt. Eine weitere sinnvolle Verpflichtung ist die Einhaltung der lizenzrechtlichen Vorschriften. Das bedeutet, dass der Tester nur kommerzielle Tools zur Durchführung der Tests verwenden darf, welche nicht illegal erworben wurden[15].

Neben diesen möglichen Pflichten sollte auch immer eine Dauer der Durchführung festgesetzt sein. Damit kann ein Unternehmen versuchte Zugriffe mit diesen Tools außerhalb des vereinbarten Zeitraums eindeutig als feindliche Angriffe identifizieren und dann strafrechtlich verfolgen.

[15] Vgl. BSI (2003), S. 33 f.

3Portscanner

In dieser Arbeit werden ausschließlich Port Scanner betrachtet, da diese als Grundlage für einen gezielten Angriff herangezogen werden können. Dabei wird beispielsweise aufgedeckt welche Ports innerhalb eines Netzwerkes geöffnet sind.

Im folgenden Abschnitt werden diese Tools genauer erläutert und auf die unterschiedlichen Methoden, welche die Tools nutzen, eingegangen. Zudem wird die getestete Software beschrieben und vorgestellt.

3.1 Definition

Das Transmission Control Protocol (TCP) und User Datagram Protocol (UDP)bilden Kommunikationsschnittstellen zwischen Systemen und basieren auf der TCP/IP Protokollfamilie. Die beiden Protokolle dienen dazu, sicherzustellen, dass der IP-Informationsfluss funktioniert. Sie kontrollieren ob die Internetprotokolle (IP) an ihrem Zielport ankommen. Jedem Teilnehmer einer Kommunikation, zum Beispiel Client und Server, werden Ports zugewiesen die eindeutig über IP und die Portnummer identifiziert werden können. Über diese Ports findet die Kommunikation zwischen Systemen statt[16].

Mit Hilfe von Portscannern werden offene und geschlossene Ports innerhalb eines Netzwerkes ermittelt und somit Schwachstellen eines Computers bzw. Systemsidentifiziert. Das Tool versucht hierbei sich nacheinander mit allen Ports eines Computers zu verbinden und zeigt im Anschluss erfolgreiche beziehungsweise negative Versuche auf. Indem der Scanner ein Paket an den entsprechenden Rechner sendet und auf dessen Antwort wartet, kann somit ausgewertet werden, ob ein Programm dieses Paket auf dem Port entgegen nimmt[17].

Durch Portscanner wird kein Angriff durchgeführt, sondern lediglich ermittelt, welche Ports geöffnet sind, indem sämtliche verfügbare Netzwerkdienste eines Remote Systems bestimmt werden[18].

Es gibt weiterführend auch Vulnerability Scanner, welche bereits eine Datenbank mit möglichen Schwachstellen mitliefern. Diese werden hier aber nicht näher beleuchtet.

---

[16] Vgl. Frisch, A. (2003), S. 193 ff.
[17] Vgl. Ballmann, B. (2012), S. 56
[18]Vgl.Rey, E./Thumann, M./Baier, D. (2005), S. 22

3.2 Methoden

Bei einem Portscan wird grundsätzlich immer versucht eine Verbindung mit einem Zielsystem aufzubauen. Als Ergebnis werden Dienste gemeldet, welche ausgeführt werden oder sich im aktiven Status (abhören) befinden. Im aktiven Status kann ein unberechtigter Nutzer aufgrund von fehlenden Konfigurationen eines Systems oder Systemen mit bekannten Sicherheitslücke Zugriff zu einem System bekommen. Dadurch können über diese Schnittstellen Anwendungen sowie das Betriebssystem ermittelt werden. Als Ziel wird dabei das Erkennen

- Von TCP- und UDP-Diensten
- Des Betriebssystem des Ziels
- Von spezifischen Anwendungen oder Versionen einer Software

Um die einzelnen Verfahren verstehen zu können, wird hier kurz das Schema des TCP-Verbindungsaufbaus, dem sogenannten „3-Way-Handshake“, beschrieben:

Im TCP-Header sind der Destination-Port sowie ein Flag-Feld (Optionsfeld) angegeben. Damit werden bestimmte Optionen im TCP aktiviert. Das Flag-Feld ist 6 Bit lang und ist ein Urgent-Pointer (URG-), Acknowledgement- (ACK-), Push- (PSH-), Reset-(RST-), Syncronization- (SYN-) oder Final- (FIN-Bit) bzw. Flag, wovon nur 3 Bit für den Prozess des Verbindungsaufbaus relevant sind: das SYN-, ACK- und RST-Bit. Das FIN-Bit ist für den Verbindungsabbau zuständig. Der Verbindungsaufbau lässt sich durch das jeweils gesetzte Bit steuern. Um nun eine Verbindung aufzubauen, werden drei Schritte durchgeführt, welche in Abbildung 1 nochmals veranschaulicht werden.

1. Zunächst wird vom Client eine Verbindungsanfrage, mit dem Destination-Port und gesetzten SYN-Bit im Header, gesendet.
2. Wenn das Zielsystem die Anfrage akzeptiert, antwortet dieser mit einem Segment in dem das SYN- sowie das ACK-Bit gesetzt ist.
3. Der Client bestätigt den Vorgang dann mit dem ACK-Bit.[19]

[19] Garleski, S. (2003)

TCP-Client
TCP-Server
Verbindungswunsch SYN (1.)
Bestätigung + Verbindungswunsch ACK + SYN (2.)
Bestätigung ACK (3.)
Datenaustausch

Abbildung 1 TCP-Verbindungsaufbau[20]

Es wird zwischen verschiedenen Verfahren vom Scanning unterschieden. Grundsätzlich können diese Methoden aber als UDP- und TCP-Scans klassifiziert werden. Zudem gibt es noch Ping-sweeps. Die zahlreichen weiteren Methoden werden nicht betrachtet, da diese selten in Portscannern implementiert werden.

Die größere Gruppe bilden die TCP- Scans. Hier gibt es folgende Scanninng Verfahren, welche im Weiteren genauer beschrieben werden:

- TCP-Connect Scan
- TCP-SYN Scan
- TCP-FIN Scan
- TCP Xmas(Tree) Scan
- TCP-Null-Scan
- TCP-ACK Scan
- TCP-Idle Scan

Der **TCP-Connect Scan** ist eine vom Zielsystem leichter zu erkennende Methode, als beispielswiese der TCP-SYN Scan. Dabei wird eine vollständige TCP-Verbindung mit einem Zielport aufgebaut, durch den Systemaufruf „connect", und ein 3-Wege-Handshake durchgeführt, wie in Abbildung 2 dargestellt. Der Aufruf wird von Web-Browsern und Netzwerk-Anwendungen genutzt. Bei dem Scan Verfahren wird die aufgebaute TCP-Verbindung vollständig beendet sobald diese nicht mehr benötigt wird.

[20] o. V. (o. J.b)

Jedoch bedeutet dies einen größeren Zeitaufwand sowie mehrere Pakete um denselben Informationsgehalt wie bei dem bereits erwähnten TCP-SYN Scan zu erhalten[21].

Abbildung 2 TCP-Connect Scan[22]

Ein sogenanntes „halb offenes Scanning“ wird bei einem **TCP-SYN Scan** durchgeführt. Dieser trägt die Bezeichnung, da keine vollständige TCP-Verbindung aufgebaut wird und diese zudem niemals abschließt. Die Funktionsweise ist wie folgt: es wird ein Paket mit gesetztem SYN-Flag an den Zielport geschickt und damit vorgetäuscht, eine echt Verbindung aufbauen zu wollen. Eine Rückmeldung in Form eines SYN/ACK bedeutet, dass der Port sich im offenen Status befindet. RST lässt darauf schließen, wie auch im unteren Teil der Abbildung 3 zu sehen ist, dass der Port geschlossen ist. Ein Port gilt dann als gefiltert, wenn nach mehrfachen Verbindungsversuchen keine Rückmeldung erfolgt oder eine ICMP-Antwort vom Typ unreachable empfangen wird. Dadurch, dass keine vollständige Verbindung aufgebaut wird, ist diese Methode unauffälliger als beispielsweise der TCP-Connect Scan[23].

Abbildung 3TCP-SYN Scan[24]

[21]McClure, S./Scambray, J./Kurtz, G. (2003), s. auch Christian Book (2012)
[22]Christian Book (2012)
[23]McClure, S./Scambray, J./Kurtz, G. (2003), s. auch Christian Book (2012)
[24]Christian Book (2012)

Diese Methode ist zuverlässig und Plattformunabhängig. Zudem werden dadurch offene, gefilterte und geschlossene Namensgebend für den **TCP-FIN Scan** ist das dabei übermittelte FIN-Paket. Dabei wird vom Zielsystem bei geschlossenem Port mit einem RST geantwortet, wie unten in der Abbildung 4 zu sehen. Bei gefilterten Ports wird die Rückmeldung „unreachable“ oder keine Meldung zurückgeliefert. Keine Rückmeldung kann jedoch auch auf einen geschlossenen Port hinweisen. Diese Methode ist allerdings nur bei UNIX-basierten TCP-IP Stacks möglich[25].

Angreifer
FIN + Port
Ziel-System
Ergebnis: Port ist offen
Angreifer
FIN + Port
RST
Ziel-System
Ergebnis: Port ist geschlossen

Abbildung 4TCP-FIN Scan[26]

Beim **TCP Xmas (Tree) Scan** werden gleich drei Flags gesetzt: FIN, URG und PUSH. Dies kann auch Abbildung 5 entnommen werden. Wie beim TCP-FIN Scan wird ein RST-Paket zurückgesendet, wenn der angesprochene Port geschlossen ist[27].

Angreifer
FYN / PSH / URG + Port
Ziel-System
Ergebnis: Port ist offen
Angreifer
FYN / PSH / URG + Port
RST
Ziel-System
Ergebnis: Port ist geschlossen

Abbildung 5TCP Xmas (Tree) Scan[28]

[25]McClure, S./Scambray, J./Kurtz, G. (2003), s. auch Christian Book (2012)
[26]Christian Book (2012)
[27]McClure, S./Scambray, J./Kurtz, G. (2003), s. auch Christian Book (2012)
[28]Christian Book (2012)

Im Gegensatz zu den bisher vorgestellten Verfahren wird bei dem **TCP-Null Scan** kein Paket an die Ports gesandt, sondern die Flaggen ausgeschalten, indem der TCP-Flag-Header auf den Wert 0 gesetzt. Dies hat jedoch wieder einen ähnlichen Effekt: es wird bei nicht erreichbaren Ports ein gesetztes RST-Flag an den Angreifer gesendet, wie in Abbildung 6 zu sehen[29].

Abbildung 6TCP-Null Scan[30]

Die Verfahren TCP-Null, Xmas sowie FIN haben den Vorteil, dass diese von einigen Firewallsystemen und paketfilternden Routern nicht erkannt werden. Außerdem sind sie unauffälliger als die bisher vorgestellten Methoden. Es werden häufig nur unzuverlässigen Ergebnisse geliefert, vor allem auf Geräten mit Microsoft Windows Betriebssystemen und Cisco, weshalb sie nur für UNIX Systeme geeignet sind.

Nicht durch Firewalls geschützte Systeme liefern sowohl für offene als auch geschlossene Ports ein TCP-Segment mit gesetztem RST Flag zurück. Das Test-Paket erreicht diese Ports, jedoch kann nicht bestimmt werden, ob sie offen oder geschlossen sind. Ports, die nicht antworten oder bestimmte ICMP-Meldungen vom Typ Unreachable zurückgeben (Type 3, Code 1, 2, 3, 9, 10 oder 13), sind gefiltert.

Mit Hilfe des **TCP-ACK Scans** ist es möglich, Sicherheitsregeln einer Firewall zu erkennen. Dabei kann dieser unterscheiden ob es sich um zustands-behaftete oder Firewall gefilterte Ports handelt. Es ist nur das ACK-Flag im TCP-Segment gesetzt, wie in Abbildung 7 dargestellt.

---

[29] McClure, S./Scambray, J./Kurtz, G. (2003), s. auchChristian Book (2012)
[30]Christian Book (2012)

Systeme welche nicht durch eine Firewall geschützt sind, liefern ein TCP-Segment mit gesetztem RST-Flag zurück, d.h. dass der Port erreicht wird, aber nicht bestimmt werden kann ob dieser offen oder geschlossen ist. Gefilterte Ports können an der Meldung „unreachable" oder am Ausbleiben einer Antwort erkannt werden[31].

Abbildung 7TCP-ACK Scan[32]

Bei dem **TCP Idle Scan**handelt es sich um einen blinden TCP-Port Scan. Hierbei wird jedoch kein Paket direkt an das Zielsystem geschickt, sondern ein Zombie-Rechner dazwischen eingesetzt. Dabei geben die Protokolldateien den Zombie-Rechner als Urheber an. Um einen solchen für einen TCP Idle Scan nutzen zu können, muss dieser eine Verbindung zum System das gescannt werden soll aufbauen können und zudem die IP Identification-Number (IPID) für den Angreifer berechenbar sein. Der Zombie-Rechner darf selbst keine TCP-Segmente generieren, denn sonst würde sich die IPID erhöhen. Deshalb sollte sich dieses am Besten im Idle (ungenutzten) Zustand befinden. Daher sind Router dafür sehr gut geeignet. Um den Scan durchführen zu können, muss die IPID des Zombie-Rechners bekannt sein.

Beim Port-Scan wird ein gefälschtes TCP-Segment mit gesetztem SYN-Bit an das Zielsystem. Hierbei wird als Quelle die IP-Adresse des Zombie-Rechners angegeben. Bei geöffnetem Port antwortet das Zielsystem mit einem SYN/ACK-Paketen. Dieses an den Zombie-Rechner gesendet, in einem TCP-Segment das RST-Flag gesetzt und an das Zielsystem zurückgesendet, denn der Zombie-Rechner hat keine Verbindung gestartet.

---

[31] McClure, S./Scambray, J./Kurtz, G. (2003) ,s. auch Christian Book (2012)
[32]Christian Book (2012)

Ist der Port geschlossen wird dem Zombie-Rechner ein RST-Paket zurückgegeben, welches dieser einfach ignoriert. Zum Abschluss des Scans fordert der Angreifer die IPID des Zombie-Rechners an. Falls diese um zwei erhöht ist, ist davon auszugehen, dass der gescannte Port des Angriffsziels geöffnet. Der Port ist geschlossen, wenn die IPID nur um eins erhöht wurde. Der Prozess kann zur Veranschaulichung der Abbildung 8 entnommen wurden[33].

Abbildung 8TCP-Idle Scan[34]

Das Verfahren ist sehr aufwändig, jedoch sehr unauffällig. Zudem werden Vertrauensbeziehungen zwischen den Rechnern aufgezeigt. Der Scan zeigt jedoch ausschließlich offene Ports aus Sicht des Zombierechners an, weshalb Ergebnisse bei mehreren Zombie-Rechnern voneinander abweichen.

Neben den TCP-Scannern gibt es einen **UDP-Scan**. Diese beinhaltet das Senden eines UDP-Pakets mit leerem Header an das zu analysierende System. In Abbildung 9 wird der Ablauf eines Scans mit UDP dargestellt. Ist der Port geschlossen, wird die Antwort ICMP Port unreachable (Typ3, Code 3) erhalten. Wenn der Port gefiltert wird, bekommt der Angreifer die Rückmeldung ICMP Port unreachable (Typ 3, Code 1, 2, 9, 10, 13).

[33]McClure, S./Scambray, J./Kurtz, G. (2003), s. auch Christian Book (2012)
[34]Christian Book (2012)

Wird mit einem UDP-Segment geantwortet, so ist der Port offen. Es kann keine gültige Aussage getroffen werden, wenn keine Rückmeldung erfolgt. UDP ist ein verbindungsloses Protokoll, wird demnach im Normalfall nicht vom Zielsystem erkannt und aufgezeichnet. Das Problem liegt dabei in der Genauigkeit sowie der Dauer des Scans. Diese hängen von vielen Faktoren ab, beispielsweise von den Systemressourcen und der Anzahl der Paketfilter die eingesetzt werden. Dies hat zur Folge, dass nur unzuverlässige Ergebnisse mit diesem Verfahren erzielt werden können[35].

Abbildung 9UDP-Scan[36]

Die Verfahren, welche mit RST-Paketen arbeiten sind bei einigen IP-Implementierungen ungünstig, da diese für alle abgefragten Ports diese zurückgeben. Die Ergebnisse können bei diesen Scans daher variieren[37].

3.3 Tools

Da diese Arbeit im Rahmen des Kompetenzcenters für Open Source entstanden ist, wurden für die Marktanalyse und die durchgeführten Tests nur Open Source Port Scanner betrachtet. Open Source bedeutet, dass die Produkte kostenfrei zur Verfügung stehen und der Quellcode der Programme offen zugänglich ist, sodass sie, wenn die dafür notwendigen Programmierkenntnisse vorhanden sind verändert und angepasst werden können.

---

[35] McClure, S./Scambray, J./Kurtz, G. (2003) , s. auch Christian Book (2012)
[36]Christian Book (2012)
[37] McClure, S./Scambray, J./Kurtz, G. (2003) , s. auch Christian Book (2012)

Es wurden die Port Scanner NMap, Nast, Strobe, Knocker und Angry IP Scanner getestet. Diese wurden ausgewählt aufgrund ihrer Aktualität, Verbreitung, vorhandener Dokumentation und Informationen. Die Produkte, welche getestet wurden, werden im nachfolgenden Abschnitt genauer vorgestellt. Alle Tests wurden auf einer Virtuellen Maschine, der Virtual Box, mit dem Betriebssystem Ubuntu durchgeführt. Dies ist eine Distribution von Linux.

3.3.1 NMap mit dem Graphical User Interface (GUI) ZenMap

NMap (Network Mapper) ist der wohl bekannteste und meist genutzte Portscanner. Das Tool kann durch die Benutzeroberfläche „ZenMap" ergänzt werden, was eine benutzerfreundliche Bedienung ermöglicht. Die Standardeinstellung, welche eine Auswahl der aufgezeigten Scan-Methoden (siehe Formular NMap) beinhaltet, bietet eine Möglichkeit der Eingrenzung bezüglich des Umfanges. So kann beispielsweise ein „Intense Scan plus UDP" oder ein „Intense Scan no ping" durchgeführt werden. Über die Option „Profil" kann zudem ein benutzerdefinierter Scan mit diversen Eigenschaften (beispielsweise TCP Scan, Target, Timing template,…) hinterlegt und durchgeführt werden. Das Resultat beinhaltet neben der NMap-Ausgabe außerdem detaillierte Informationen wie zum Beispiel über die Netzstruktur und Rechner-Details. Dieses kann wiederum innerhalb NMap gespeichert und zu einem späteren Zeitraum erneut aufgerufen werden.[38]

Version	NMap 6.40, ZenMap 6.40.1
Letztes Update	30.07.2013 NMap;
Größe	7,9 MB
Plattformen	• Windows NT, 2000, XP, Server 2003, Server 2008, Vista, 7 • Linux • Mac OS X, Mac OS X/Intel
Funktionsumfang	
- **Methoden**	• TCP-Connect Scan • TCP-SYN-Scan • TCP-FIN Scan • TCP-NULL Scan • TCP-ACK Scan • TCP XmasTree Scan • TCP-Idle Scan • ICMP-Ping-sweep

[38] Vgl. o. V. (o. J.c)

	• UDP-Scan • TCP-Window-Scan • TCP-Maimon-Scan • Benutzerdefinierter TCP-Scan • IP-Protokoll-Scan • FTP-Bounce-Scan
- **Anpassbarkeit**	Vorbelegte Methoden (siehe oben) können ausgewählt werden. Profilverwaltung durch Profileditor: benutzerdefinierte Scans können hinterlegt, gespeichert und durchgeführt werden (z.B. Einstellung: Target, Scan, Ping, Scripting, Source, Other Timing,…)
- **Beschränkungen**	Nur als Root Benutzer in vollem Umfang benutzbar, sonst Einschränkungen
- **Bedienbarkeit**	Durch die Oberfläche ZenMap leicht und übersichtlich zu bedienen, verschiedene Ansichten des Scans möglich
Oberfläche:	
Beschreibung der Oberfläche	Bei der Zieleingabe handelt es sich um die IP Adresse, welche auf offene oder geschlossene Ports überprüft werden soll. In dem Profil kann eine der oben genannten Methoden ausgewählt werden

Ergebnis: Beispiel Intense Scan, all TCP ports	Zenmap Scan Werkzeuge Profil Hilfe Ziel: 10.02.2.15 Profil: Intense scan, all TCP ports Scan Abbrechen Befehl: nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 10.02.2.15 Rechner Dienste | Nmap-Ausgabe Ports / Rechner Netzstruktur Rechner-Details Scans Betriebssystem | nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 10.02.2.15 Details Initiating Traceroute at 13:55 Completed Traceroute at 13:55, 3.02s elapsed Initiating Parallel DNS resolution of 1 host. at 13:55 Completed Parallel DNS resolution of 1 host. at 13:55, 1.09s elapsed NSE: Script scanning 10.2.2.15. NSE: Script Scanning completed. Nmap scan report for 10.2.2.15 Host is up (0.042s latency). All 65535 scanned ports on 10.2.2.15 are filtered Too many fingerprints match this host to give specific OS details Network Distance: 2 hops TRACEROUTE (using port 21/tcp) HOP RTT ADDRESS 1 ... 2 4.79 ms 10.2.2.15 Read data files from: /usr/share/nmap OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 3712.71 seconds Raw packets sent: 132990 (5.848MB) | Rcvd: 1683 (67.344KB) Rechner filtern Zenmap Scan Werkzeuge Profil Hilfe Ziel: 10.02.2.15 Profil: Intense scan, all TCP ports Scan Abbrechen Befehl: nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 10.02.2.15 Rechner Dienste | Nmap-Ausgabe Ports / Rechner Netzstruktur Rechner-Details Scans Betriebssystem | Port Protokoll Status Dienst Version 67 udp open Rechner filtern
Beschreibung des Ergebnisses	Die Screenshots stellen das Ergebnis des Intense Scan all TCP dar. Insgesamt wurden 65535 Ports getestet. Das Resultat kann in verschiedenen Darstellungsweisen angeschaut werden.
Weitere Einzelheiten vom Ergebnis:	StartingNmap 5.21 (http://nmap.org) at 2014-01-06 12:53 CET NSE: Loaded 36 scripts for scanning. Initiating Ping Scan at 12:53

	Scanning 10.2.2.15 [8 ports] Completed Ping Scan at 12:53, 0.09s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 12:53 Completed Parallel DNS resolution of 1 host. at 12:53, 1.07s elapsed Initiating SYN Stealth Scan at 12:53 Scanning 10.2.2.15 [65535 ports] SYN Stealth Scan Timing: About 2.46% done; ETC: 13:14 (0:20:32 remaining) Increasing send delay for 10.2.2.15 from 0 to 5 due to 11 out of 19 dropped probes since last increase. Increasing send delay for 10.2.2.15 from 5 to 10 due to 11 out of 11 dropped probes since last increase. SYN Stealth Scan Timing: About 2.56% done; ETC: 13:33 (0:38:46 remaining) SYN Stealth Scan Timing: About 2.93% done; ETC: 13:45 (0:50:18 remaining) SYN Stealth Scan Timing: About 4.97% done; ETC: 13:34 (0:38:33 remaining) SYN Stealth Scan Timing: About 5.18% done; ETC: 13:42 (0:46:03 remaining) SYN Stealth Scan Timing: About 6.73% done; ETC: 13:40 (0:43:12 remaining) SYN Stealth Scan Timing: About 7.65% done; ETC: 13:46 (0:48:18 remaining) SYN Stealth Scan Timing: About 9.43% done; ETC: 13:41 (0:43:12 remaining) SYN Stealth Scan Timing: About 10.08% done; ETC: 13:44 (0:45:55 remaining) SYN Stealth Scan Timing: About 11.96% done; ETC: 13:42 (0:43:04 remaining) SYN Stealth Scan Timing: About 12.72% done; ETC: 13:45 (0:45:38 remaining) SYN Stealth Scan Timing: About 14.50% done; ETC: 13:43 (0:42:45 remaining) SYN Stealth Scan Timing: About 24.23% done; ETC: 13:46 (0:40:11 remaining)

	SYN Stealth Scan Timing: About 31.35% done; ETC: 13:48 (0:37:20 remaining) SYN Stealth Scan Timing: About 38.49% done; ETC: 13:49 (0:34:35 remaining) SYN Stealth Scan Timing: About 44.55% done; ETC: 13:50 (0:31:45 remaining) SYN Stealth Scan Timing: About 50.01% done; ETC: 13:51 (0:28:51 remaining) SYN Stealth Scan Timing: About 55.76% done; ETC: 13:52 (0:25:55 remaining) adjust_timeouts2: packet supposedly had rtt of 8583165 microseconds. Ignoring time. adjust_timeouts2: packet supposedly had rtt of 8583165 microseconds. Ignoring time. SYN Stealth Scan Timing: About 61.23% done; ETC: 13:52 (0:22:56 remaining) SYN Stealth Scan Timing: About 66.42% done; ETC: 13:53 (0:19:58 remaining) SYN Stealth Scan Timing: About 71.61% done; ETC: 13:53 (0:16:59 remaining) SYN Stealth Scan Timing: About 76.98% done; ETC: 13:54 (0:13:57 remaining) adjust_timeouts2: packet supposedly had rtt of 8196579 microseconds. Ignoring time. adjust_timeouts2: packet supposedly had rtt of 8196579 microseconds. Ignoring time. SYN Stealth Scan Timing: About 82.11% done; ETC: 13:54 (0:10:53 remaining) adjust_timeouts2: packet supposedly had rtt of 8280362 microseconds. Ignoring time. adjust_timeouts2: packet supposedly had rtt of 8280362 microseconds. Ignoring time. SYN Stealth Scan Timing: About 87.23% done; ETC: 13:54 (0:07:48 remaining) SYN Stealth Scan Timing: About 92.29% done; ETC: 13:54 (0:04:43 remaining) SYN Stealth Scan Timing: About 97.37% done; ETC: 13:55

	(0:01:37 remaining) Completed SYN Stealth Scan at 13:55, 3696.25s elapsed (65535 total ports) Initiating Service scan at 13:55 Initiating OS detection (try #1) against 10.2.2.15 Retrying OS detection (try #2) against 10.2.2.15 Initiating Traceroute at 13:55 Completed Traceroute at 13:55, 3.02s elapsed Initiating Parallel DNS resolution of 1 host. at 13:55 Completed Parallel DNS resolution of 1 host. at 13:55, 1.09s elapsed NSE: Script scanning 10.2.2.15. NSE: Script Scanning completed. Nmap scan report for 10.2.2.15 Host is up (0.042s latency). All 65535 scanned ports on 10.2.2.15 are filtered Too many fingerprints match this host to give specific OS details Network Distance: 2 hops TRACEROUTE (using port 21/tcp) HOP RTT ADDRESS 1 ... 2 4.79 ms 10.2.2.15 Read data files from: /usr/share/nmap OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 3712.71 seconds Raw packets sent: 132990 (5.848MB) | Rcvd: 1683 (67.344KB)
Performance	Intense scan, all TCP ports: 3712.71 seconds
Bemerkungen .	Kann im Terminal oder mit Oberfläche ZenMapdurchgeführt werden. Einfache Installation und Handhabung, sehr übersichtlich durch die Grafische Oberfläche ZenMap. Auswahl der unterschiedlichen Methoden und verschiedene Ausgabenmöglichkeiten. Scans können gespeichert und wieder aufgerufen werden. Schneller, einfacher Vergleich der Ergebnisse.

Tabelle 1 Formular zu NMAP

3.3.2 Nast

Nast (Network AnalizerSniffer Tool) ist ein Tool zum „sniffen“ von Paketen, sowie ein LAN-Analysierer, welches ohne Benutzeroberfläche, also anhand des Terminals bedient wird. Neben diversen Funktionen, wie zum Beispiel „find-gateway“ zum Auffinden von möglichen Internet-Gateways oder „reset-connection“ um eine bestehende Verbindung zu trennen“, bietet Nast das Durchführen eines “port-scans“, sowie ein „multi-port-scans“ an. Beide Scan-Möglichkeiten basieren auf TCP-Scans, welche über die SYN-FLAG Methode durchgeführt werden (siehe hierzu Kapitel 3.2). Auch hier ist eine Ausgabe in Logfiles (zum Beispiel in ascii oder ascii-hex Format) durchführbar.[39]

Nast (Network Analizer Sniffer Tool)

Version	Nast 0.2.0-5.2
Erscheinungsjahr	16.02.2004
Größe	217,1 kB
Plattformen	Linux
Funktionsumfang	
- **Methoden**	• TCP-SYN-Scan
- **Anpassbarkeit**	-
- **Beschränkungen**	Muss als Root Benutzer ausgeführt werden
- **Schnittstellen**	Ausgabe in txt-Datei möglich [--ldfilename]
Bedienbarkeit	Über Terminal, keine vertieften Linux Kenntnisse nötig
Oberfläche	heike@heike-VirtualBox: ~ heike@heike-VirtualBox:~$ nast -S Nast V. 0.2.0 You must be root, Sorry heike@heike-VirtualBox:~$ sudo nast -S [sudo] password for heike: Nast V. 0.2.0 Port Scanner extremes Insert IP to scan : 10.0.2.15
Beschreibung der Oberfläche	Der Portscanner wird im Terminal ausgeführt. Wie in dem Screenshot ersichtlich wird Nast durch den Befehl „nast –S“

[39] Vgl. o. V. (o. J.d)

	gestartet. Zu beachten sind die Benutzerrechte, da der Scanner nur als „Root“ ausgeführt werden kann.
Ergebnis	heike@heike-VirtualBox: ~ Filtered 83 unknown SYN packet timeout(**) Filtered 84 unknown SYN packet timeout(**) Filtered 85 unknown SYN packet timeout(**) Filtered 86 unknown SYN packet timeout(**) Filtered 87 link SYN packet timeout(**) Open 88 kerberos None Open 89 unknown None Open 90 unknown None Open 91 unknown None Open 92 unknown None Filtered 93 unknown SYN packet timeout(**) Filtered 94 unknown SYN packet timeout(**) Filtered 95 supdup SYN packet timeout(**) Filtered 96 unknown SYN packet timeout(**) Filtered 97 unknown SYN packet timeout(**) Filtered 98 linuxconf SYN packet timeo ut(**) Open 99 unknown None All the other 1 ports are in state closed (**)Possible DROP rule in the firewall Scanning terminated on Jan 15 15:03:11 heike@heike-VirtualBox:~$
Beschreibung des Ergebnisses	Nachdem der Portscanner gestartet wurde, wird der Nutzer aufgefordert die IP-Adresse einzugeben. Im Anschluss muss eine „Range“ eingegeben werden, d.h. der Umfang der zu untersuchenden Ports. Durch „Enter“ wird der Scan gestartet und offene und gefiltert Port werden aufgeführt.
Performance	Keine Zeitangabe
Bemerkungen	Leichte Installation über Debian Package, einfache Handhabung und übersichtliche Ausgabe. Keine Updates vorhanden, letzte Version wurde 2004 veröffentlicht. Tool ist nicht weitverbreitet und wird nur von vereinzelten Anbietern zum Download bereitgestellt.

Tabelle 2 Formular zu Nast

3.3.3 Knocker

Knocker ist ein TCP-Sicherheitsportscanner der in C geschrieben wurde. Er scannt Hosts und benennt die auf ihnen gestarteten Services.[40]

Knocker Portscanner

Version	0.7.1 (Internetseite der Hersteller)
letztes Update	24. Mai 2002
Größe	716,7 MB
Plattformen	• Linux

[40] Vgl. o. V. (o. J. e):

	• FreeBSD • HP-UX • Windows9x/2000/NT • OpenBSD
Funktionsumfang	
- **Methoden**	Nur TCP-Scan der Ports, keine weiteren Funktionen
- **Anpassbarkeit**	Nur die Ausgabe kann angepasst werden
- **Beschränkun-gen**	Nur eine Scanmöglichkeit, sonst keine Features
- **Schnittstellen**	Ein Logfile kann erstellt werden.
Bedienbarkeit	Nach der Installation ist die Bedienung über einfache Befehle möglich, es wird außerdem auch eine Hilfe angeboten.
Oberfläche	**Abbildung 10 Screenshot des GTK-Knockers**[41]

[41] entnommen aus: o. V. (o. J. f):

Beschreibung der Oberfläche	Das ist ein Bild der Oberfläche des nicht getesteten GTK-Knocker, sonst wird der Scanner über Terminal gestartet Hier gibt man oben zunächst den zu scannenden Host und die Ports an. Die Buttons für das Starten und Beenden des Scans sind auch in dieser Zeile. In der nächsten Zeile gibt man sowohl an ob eine Log-Datei erstellt werden soll und auch wohin diese gespeichert werden soll. Das mittlere Feld ist das Ergebnis des Scans als nicht konsolenartige Ausgabe. Das untere Feld bietet das Ergebnis als Konsolenausgabe. In beiden Feldern stehen die Portnummern der offenen Ports und welcher Service auf ihnen läuft. Rechts unten gibt es einen Fortschrittsbalken. Die Ausgabe über die Konsole kann im unteren Screenshot gesehen werden.
Ergebnis	|--=| k n o c k e r -- t h e -- n e t -- p o r t s c a n n e r |=- - started by user blubb on Tue Jan 21 06:36:14 2014 - hostname to scan: 10.0.2.15 - resolved host ip: 10.0.2.15 - - scan from port: 1 - - - scan to port: 1024 - - - - scan type: tcp connect +=- s c a +=- c o m p - scanned host name: 10.0.2.15 IP: 10.0.2.15 - found 0 open ports in a total of 1024 ports scanned. - port scan completed in 0.02 seconds.
Beschreibung des Ergebnisses	Diese Ausgabe stammt aus der konsolenbasierten Version des Knocker Portscanners. Das Ergebnis des Scans ist eine Auflistung der offenen Ports. Außerdem werden nochmals die Eingabedaten, und die Startzeit angezeigt. Des Weiteren werden die Ausführzeit, der Scantyp, der ausführende User und auch die Anzahl gescannter Ports angezeigt. Die Funktionen sind wie bei der graphischen Oberfläche beschrieben, werden aber über Befehle aufgerufen. In dem obigen Beispiel wurden in den ersten 1024 Ports keine offenen Ports erkannt und daher gibt es auch keine Auflistung der Ports.

Performance	Wird variieren je nach Anzahl gescannter Ports.
Bemerkungen	Dieser Scanner ist von der Bedienung recht einfach und vom Funktionsumfang sehr klein gehalten. Er beschränkt sich wirklich nur auf einen einfachen Scan der Ports und die Ausgabe der offenen Ports. Das Betriebssystem Ubuntu verfügt über ein Softwarecenter über das der Scanner sehr einfach zu installieren ist. Die Installation über das Terminal ist für nicht erfahrene Terminalnutzer nicht unbedingt einfach, aber die Installationsanleitung des Scanners bietet einen guten ersten Anhaltspunkt.

Tabelle 3 Formular zu Knocker

3.3.4 Angry IP Scanner

Der Angry IP Scanner ist ein Netzwerk Scanner, mit welchem sich IP-Adressen, Mac-Adressen und offene Ports ermitteln lassen. Das Tool „pingt" hierbei die zuvor definierte IP-Adresse an und prüft ob diese aktiv ist. Der Umfang, beziehungsweise der IP- Bereich, kann dazu von dem Nutzer frei gewählt werden. Das Resultat kann in eine TXT-, XML, IP-Port-Liste oder CSV-Datei ausgegeben werden. Die Benutzeroberfläche erlaubt eine einfache und übersichtliche Handhabung. Durch weitere Plug-ins lässt sich der Umfang der Funktionen erweitern und anpassen.[42]

Version	ipscan 3.2.1-1
Letztes Update	
Größe	972,8 kB
Plattformen	Linux, Windows
Funktionsumfang	
- **Methoden**	• TCP-SYN-Scan • ICMP-Ping-sweep • UDP-Scan
- **Anpassbarkeit**	IP Range lässt sich eingeben, Random, IP List File, sonstige benutzerdefinierte Einstellungen wie z.B. Display: nur offene Ports anzeigen,…
- **Beschränkungen**	-
- **Schnittstellen**	Exportieren als TXT oder CSV-Datei möglich
Bedienbarkeit	Leichte Bedienbarkeit durch GUI

[42] Vgl. o. V. (2013)

Oberfläche	
Beschreibung der Oberflächen	Unter den Feldern „IP Range“ und „to“ wird die zu untersuchende IP Adresse eingegeben. Durch klicken auf „Start“ wird der Scan ausgeführt.
Ergebnis	
Beschreibung des Ergebnisses	Nachdem der Scan erfolgreich durchgeführt wurde, werden die Ports in der Ausgabeoberfläche angezeigt. Durch die farbliche Markierung ist zu erkennen welche Ports offen (grün), gefiltert (blau) und geschlossen (rot) sind. Des Weiteren wird über das Fenster „Scan Statistics“ die Dauer des Scans, die Durchschnittliche Dauer pro Host, die IP Range und die gescannten Hosts sowie die Aktiven Hosts angezeigt.
Performance	Anzeige der Dauer 1,6Sec
Bemerkungen	Einfache Installation und Handhabung

Tabelle 4 Formular zu Angry IP Scanner

3.3.5 Strobe

Strobe ist ein schnelles und zuverlässiges Tool, welches jedoch bereits im Jahr 1995 von Julian Assange im Quellcode C geschrieben wurde. Das Werkzeug nutzt TCP-Portscanning Utilities um alle aktiven Ports aufzulisten[43].

Version	1.06
Letztes Update	1999
Größe	297,4 kB
Plattformen	Linux, Windows
Funktionsumfang	
- **Methoden**	TCP-Scanning Methoden
- **Anpassbarkeit**	Einige Optionen dafür möglich (dafür Fachkenntnisse notwendig), z.B. nur einen bestimmten Port Scannen
- **Beschränkungen**	Nur TCP Scanning möglich, kein UDP Scanning, es wird kein vollständiges Bild geliefert, nur offene Ports sichtbar
- **Schnittstellen**	Als file speicherbar
Bedienbarkeit	Einfach unter terminal, keine besonderen Kenntnisse möglich
Oberfläche	Keine GUI vorhanden, nur Terminal -rw------- 1 nemo nemo 1770 Jan 23 13:20 .ICEauthority drwxr-xr-x 3 nemo nemo 4096 Dez 18 13:45 .local/ drwx------ 3 nemo nemo 4096 Dez 18 13:45 .mission-control/ drwx------ 4 nemo nemo 4096 Dez 18 13:46 .mozilla/ drwxr-xr-x 2 nemo nemo 4096 Dez 18 13:45 Musik/ drwxr-xr-x 2 nemo nemo 4096 Dez 18 13:45 Öffentlich/ -rw-r--r-- 1 nemo nemo 675 Dez 12 22:41 .profile drwx------ 2 nemo nemo 4096 Jan 23 13:20 .pulse/ -rw------- 1 nemo nemo 256 Dez 18 13:45 .pulse-cookie drwxr-xr-x 2 nemo nemo 4096 Dez 18 13:45 Videos/ drwxr-xr-x 2 nemo nemo 4096 Dez 18 13:45 Vorlagen/ -rw------- 1 nemo nemo 60 Jan 23 13:20 .Xauthority -rw------- 1 nemo nemo 8796 Jan 23 13:21 .xsession-errors -rw------- 1 nemo nemo 101529 Jan 17 15:00 .xsession-errors.old
Beschreibung der Oberflächen	-

[43] McClure, S./Scambray, J./Kurtz, G. (2003)

Ergebnis	-VirtualBox: ~ ng UP BROADCAST RUNNING MULTICAST MTU:1500 Metrik:1 RX-Pakete:152816 Fehler:0 Verloren:0 Überläufe:0 Fenster:0 TX-Pakete:74952 Fehler:0 Verloren:0 Überläufe:0 Träger:0 Kollisionen:0 Sendewarteschlangenlänge:1000 RX-Bytes:144429426 (144.4 MB) TX-Bytes:5376870 (5.3 MB) lo Link encap:Lokale Schleife inet Adresse:127.0.0.1 Maske:255.0.0.0 inet6-Adresse: ::1/128 Gültigkeitsbereich:Maschine UP LOOPBACK RUNNING MTU:65536 Metrik:1 RX-Pakete:632 Fehler:0 Verloren:0 Überläufe:0 Fenster:0 TX-Pakete:632 Fehler:0 Verloren:0 Überläufe:0 Träger:0 Kollisionen:0 Sendewarteschlangenlänge:0 RX-Bytes:99835 (99.8 KB) TX-Bytes:99835 (99.8 KB) nemo@nemo-VirtualBox:~$ strobe 10.0.2.15 strobe 1.06 (c) 1995-1999 Julian Assange <proff@iq.org>. nemo@nemo-VirtualBox:~$ sudo strobe 10.0.2.15 [sudo] password for nemo: strobe 1.06 (c) 1995-1999 Julian Assange <proff@iq.org>. 10.0.2.15 42090 unassigned unknown 10.0.2.15 55585 unassigned unknown nemo@nemo-VirtualBox:~$
Beschreibung des Ergebnisses	Der Test der auf der virtuellen Maschine durchgeführt wurde, hat nur zwei Ports mit dem Status unbelegt als Ergebnis geliefert. Wie in der Abbildung zu sehen ist wird vorne immer die IP-Adresse des Hosts angegeben. Da dem Scanner nichts weiter über die gezeigten Ports weiß, weicht die Darstellung etwas von den Erkannten Ports ab. Denn der IP-Adresse folgt, wie im Beispiel unten, der Dienst der darüber läuft und die Nummer des Ports. Dahinter steht das Protokoll und dann eine kurze Beschreibung des Ports, beispielsweise könnten Zeilen wie folgt aussehen: 192.168.1.10 ssh 22/tcp Secure Shell
Performance	Keine Angabe
Bemerkungen	Arbeitet schnell und zuverlässig, erster Open Source Port Scanner, von Julian Assange

Tabelle 5 Formular zu Strobe

4 Marktanalyse

4.1 Definition

Eine Marktanalyse ist eine Untersuchung eines Marktes. Dabei werden sowohl Konsument als auch der Wettbewerb betrachtet. Es wird die herrschende Marktsituation dargestellt. Diese Betrachtung kann entweder auf den gesamten Markt oder nur auf ein einzelnes Teilsegment des Marktes vorgenommen werden. Die wissenschaftliche Arbeit bezieht sich demnach auf ein bestimmtes Segment des Marktes. Dieser umschließt Security Check Tools und ins besondere die Portscanner.

Eine Marktanalyse hat das Ziel, möglichst viele Informationen über den Markt zu bestimmen. Diese sind unter anderem

- Marktpotential
- Marktvolumen
- Aktuelles und erwartetes Marktwachstum
- Aktuelle und erwartete Marktanteile von verschiedenen Anbietern
- Marktverhalten (Nachfrage und Angebot)

Marktanalyse zählt als Teilgebiet der Marktforschung. Sie bezieht sich aber nur auf einen einzelnen Zeitpunkt. D.h. es wird eine Bestandsaufnahme des Marktes vorgenommen um dadurch Auskunft über die Strukturen zu treffen.

4.2 Kriterienkatalog

Der Kriterienkatalog beschreibt alle relevanten Kriterien, die zur Bestimmung einer geeigneten Software, eines geeigneten Tools oder System betrachtet werden. Mit Hilfe dieses Dokuments wird eine Grundlage für die Abstimmung und Entscheidung geschaffen.

Ein Auswahlverfahren sollte für ein Unternehmen keinen großen Aufwand bedeuten. Aus diesem Grund werden nur notwendige und nachvollziehbare Daten betrachtet. Demnach ist der Kriterienkatalog sachdienlich aufgebaut. D. h. das nicht die Vollständigkeit, sondern das Gewicht der Kriterien als Qualitätsmerkmal gilt.

Ein Kriterienkatalog lässt sich im Allgemeinen in vier Bereiche einteilen. Diese sind

- Bereich 1: Kostenrahmen und Rahmenbedingungen
- Bereich 2: Funktionale Anforderungen (speziell auf einen Bereich z.B. Außendienst)
- Bereich 3: Branchenspezifische Funktionalitäten
- Bereich 4: Anbieterbezogene Kriterien

Im Folgenden werden diese vier Bereiche am Beispiel der Portscanner angewendet.

Bereich Eins. Der Kostenrahmen spielt im Beispiel der Portscanner keine Rolle, da es sich bei den zur Auswahl stehenden Tools um Open Source Produkte handelt, welche keine Kosten für den Anwender verursachen. Die funktionalen und systematischen Rahmenbedingungen beziehen sich im Allgemeinen auf die Unternehmensstruktur und an die zukünftigen Anforderungen eines Unternehmens. Im gewählten Beispiel werden diese folgendermaßen festgelegt. Es muss sich bei den Tools um Open Source Produkte handeln, welche auf einer Linux Umgebung lauffähig sind.

Der zweite Bereich bestimmt die funktionalen Anforderungen. Im Fall der Portscanner ist das unter anderem die Anzeige der Ergebnisse, d. h. welche Ports sind offen bzw. geschlossen.

Die branchenspezifischen Funktionalitäten betreffen allgemeingültige Funktionen und Methoden für den speziellen Geschäftszweig. Das kann zum Beispiel ein Mindesthaltbarkeits-Verzeichnis für einen Lebensmittelbetrieb sein. Dieser muss individuell festgelegt werden und wird hier daher nicht näher spezifiziert.

Der vierte Bereich bezieht sich auf Kriterien, die speziell einem Anbieter zugeordnet sind. Dabei kann eine generelle Leistungsfähigkeit bestimmt werden. Diese kann zum Beispiel mit Hilfe der letzten Aktualisierung bestimmt werden. Liegt diese über einen Zeitraum von 3 Jahren zurück, kann davon ausgegangen werden, dass der Support eingestellt wurde.

Anhand dieser und weiteren gesammelten Daten wurde ein Kriterienkatalog erstellt.

		NMap	Nast	Angry IP Scanner	Knocker	Strobe
Methoden	TCP-Connect Scan	**X**			**X**	**?**
	TCP-SYN Scan	**X**	**X**	**X**		**?**
	TCP-FIN Scan	**X**				**?**
	TCP-Null Scan	**X**				**?**
	TCP-ACK Scan	**X**				**?**
	TCP XmasTree Scan	**X**				**?**
	TCP-Idle Scan	**X**				**?**
	ICMP-Ping-sweep	**X**		**X**		
	UDP-Scan	**X**		**X**		
	Sonstige	**X**	**X**	**X**		
Bestimmung Range		JA	JA	JA	JA	JA
Plattformen	Linux	JA	JA	JA	JA	JA
	Windows	JA	NEIN	JA	JA	JA
Ergebnisdokumentation		JA	JA	JA	JA	JA
Größe		7,9 MB	217,1 KB	972,8 KB	716,7MB	
Oberfläche	GUI	JA	NEIN	JA	JA	NEIN
	Terminal	JA	JA	NEIN	JA	JA
Ergebnis	Offene Ports	JA	JA	JA	JA	JA
	Geschlossene Ports	JA	NEIN	JA	NEIN	NEIN
Aktualität		07/2013	02/2004	k.A	05/2002	1999

Tabelle 6 Kriterienkatalog

Die im Katalog aufgezählten Kriterien werden im Folgenden Erläutert. Der UDP und TCP-Scan zählt zu den Grundfunktionen eines Portscanners. Um alle Ports zu finden müssen beide Funktionen von dem Tool ausgeführt werden. Der Ping ist eine dritte Möglichkeit um die Ports zu finden, welche effektiv und damit Erfolgreich bei der Suche nach Ports ist. Der Range trifft eine Aussage über den Umfang des Durchlaufs. Ist es möglich diesen zu bestimmen kann nur ein bestimmter Teil kontrolliert werden. Das hat den Vorteil, dass nicht bei jedem Test der gesamte Bereich durchsucht werden muss. Damit spart der Tester viel Zeit und kann gewisse Bereiche nach einer Verbesserung noch einmal scannen.

Bei den Plattformen wurden Linux und Windows genauer betrachtet. Dabei handelt es sich um die bekanntesten Betriebssysteme. Diese sind somit auch in Unternehmen am häufigsten im Einsatz. Das Tool kann durch die Erfahrung einfach installiert und durchgeführt werden. Die Dokumentation eines Tools hilft dem Anwender einen Überblick über dieses zu bekommen. Das Tool wird entweder mit Hilfe des Terminals oder mit einer eigenen GUI durchgeführt. Die GUI bietet den Vorteil, dass auch unerfahrene Anwender die Tools einsetzen können. Das Ergebnis macht eine Aussage über die Genauigkeit der Tools. Bei der Aktualität können Rückschlüsse auf den Support getroffen werden.

Anhand dieser Kriterien kann ein Unternehmen oder ein Tester sich nun für einen Portscanner entscheiden. Die Entscheidung der Projektgruppe und weitere Erkenntnisse werden im folgenden Kapitel beschrieben.

4.3Ergebnis und Bewertung

Aus dem Kriterienkatalog kann nun ein endgültiges Ergebnis abgeleitet werden. Die Erfüllung der Kriterien ist noch einmal grafisch in der folgenden Abbildung dargestellt.

Abbildung 11 Erfüllte Kriterien im Katalog

Der Katalog enthält achtzehn zu wertende Kriterien. Bevor eine Entscheidung für ein Tool getroffen wird, sollten mehrere Faktoren betrachtet werden. Diese sind zum Beispiel

- Fachwissen des Benutzers
- Wahl der Methode
- Integriertes Betriebssystem
- Gewünschtes Ergebnis

Mit Hilfe dieser Punkte kann nun die Situation des Auftraggebers festgelegt werden. Zum Beispiel möchte ein kleines Unternehmen einen Penetrationstest durchführen. Der Tester hat geringes Fachwissen und möchte einen TCP SYN Scan durchführen. Er besitzt einen Laptop mit einem Windows Betriebssystem. Für Ihn würde sich auf Grund der bestehenden Faktoren der NMap oder der Angry IP Scanner anbieten.

		NMap	Nast	Angry IP Scanner	Knocker	Strobe
Methoden	TCP-Connect Scan	**X**			**X**	**?**
	TCP-SYN Scan	**X**	**X**	**X**		**?**
	TCP-FIN Scan	**X**				**?**
	TCP-Null Scan	**X**				**?**
	TCP-ACK Scan	**X**				**?**
	TCP XmasTree Scan	**X**				**?**
	TCP-Idle Scan	**X**				**?**
	ICMP-Ping-sweep	**X**		**X**		
	UDP-Scan	**X**		**X**		
	Sonstige	**X**		**X**		
Plattformen	Linux	**X**	**X**	**X**	**X**	**X**
	Windows	**X**		**X**	**X**	**X**
Fachwissen	Gering	**X**		**X**	**X**	
	Hoch	**X**	**X**		**X**	**X**
Ergebnis	Offene Ports	**X**	**X**	**X**	**X**	**X**
	Geschlossene Ports	**X**		**X**		

Tabelle 7 Tabelle zu geeigneten Tools

Ein Tool eignet sich für vielfältige Anforderungen. Dabei handelt es sich um NMap. Es kann die meisten Methoden umsetzen und unabhängig von dem verwendeten Betriebssystem installiert werden. Die Anwendung gestaltet sich unkompliziert und das Ergebnis enthält sowohl geschlossene als auch offene Ports.

An zweiter Stelle befindet sich der Angry IP Scanner. Folgend kommt Strobe, Knocker und der ungeeignetste Portscanner ist Nast.

5 Fazit

Wie bereits zuvor beschrieben, dienen Penetrationstests zur Aufdeckung von Sicherheitslücken innerhalb eines Netzwerkes. Durch die ständige wachsende Nutzung von IT-Systemen und der damit verbundenen Daten rückt dieses Thema immer mehr in den Fokus. Auch die Gewährleistung von gesetzlichen Sicherheitsbestimmungen trägt dazu bei, dass Penetrationstests für ein Unternehmen unabdingbar sind. Das Ziel dieser Projektarbeit war es eine Marktstudie über jene Penetrationstests durchzuführen. Der Schwerpunkt wurde auf Tools gesetzt, welche zum Scannen von Ports dienen, sowie als Open Source Softwarezur Verfügung gestellt werden.

Zunächst wurde eine erste Auswahl bezüglich der Tools getroffen und deren Methoden genauer untersucht. Im Anschluss sind diese Portscanner auf einer virtuellen Maschine (Betriebssystem Linux – Ubuntu) installiert und getestet worden. Anhand der ermittelten Methoden und weiteren Gesichtspunkten konnte der Kriterienkatalog erstellt werden. Die Testergebnisse und die Dokumentation der Tools dienten hierbei als Grundlage für die jeweiligen Resultate.

Das Ergebnis der Arbeit zeigt, dass sich besonders NMap als Portscanner eignet, da durch dieses Tool alle untersuchten Scanning-Methoden abgedeckt werden konnten. Zudem sind die Benutzerfreundlichkeit, die Aktualität und die Verbreitung weitere Faktoren welche für NMap sprechen. Andere Portscanner, wie zum Beispiel „Angry IP Scanner“ und „Knocker“, begrenzen sich im Vergleich lediglich auf eine, beziehungsweise zwei Methoden. Auch ist die Nutzung des Tools ein wichtiger Aspekt, welcher zu berücksichtigen ist. Bietet ein Scanner nur eine Nutzung durch das Terminal, sind hierbei grundlegende Kenntnisse für das jeweilige Betriebssystem nötig. Vor allem in Bezug auf die Installation der Tools sind Linux Kenntnisse notwendig, da diese teilweise nicht über das Software Center möglich ist. Diese müssen über das Terminal nach mitgelieferter Installationsanleitung, welche nicht immer einfach zu verstehen und umzusetzen ist, installiert werden.

Anhand des ermittelten Ergebnisses kann ein Unternehmen eine Auswahl der benötigten Methoden treffen und sich somit auf einen entsprechenden Portscanner begrenzen. Diese müssen jedoch je nach Anforderung des Unternehmens ausgewählt werden. Zudem sollte genügend Wissen vorhanden sein, um das Ergebnis des Penetration Tests auswerten zu können. Zwar werden keine besonderen Kenntnisse zum Durchführen eines solchen Tests benötigt, jedoch sollten auch immer rechtliche Aspekte, eines solchen Tests betrachtet werden. Eine Erweiterung des Kriterienkatalogs durch neu entwickelte Tools ist jederzeit möglich.

Anhang

Quellenverzeichnisse

Literaturverzeichnis

Adams, K. / Agesen, O. (2006): A Comparison of Software and Hardware Techniques for x86 Virtualization, in: Proceedings of the 12th international conference on Architectural support for programming languages and operating systems, Oktober 2006

Ballmann, B. (2012): Network Hacks - Intensivkurs,Angriff und Verteidigung mit Python, in: Xpert.press, Berlin, Heidelberg: Springer Berlin Heidelberg

BSI(2003): Bundesamt für Sicherheit in der Informationstechnik - Studie Penetrationstests, Bonn

Freiling F./Liebchen J. : Iterative Kompromittierungsgraphverfeinerung als methodische Grundlage für Netzwerkpenetrationstests

Frisch, A. (2003): Unix-System-Administration, Dt. Ausg. der 3. Aufl., 2. Aufl, Köln: O'Reilly

McClure, S./ Scambray, J./ Kurtz, G. (2003): Das Anti-Hacker-Buch, [live hack im US-Original ; wireless hacking ; SQL injection, fuzzing, cross site scripting], 4. Aufl, Bonn: Mitp

Rey, E./Thumann, M./ Baier, D. (2005): Mehr IT-Sicherheit durch Pen-Tests, Optimierung der IT-Sicherheit durch gelenktes "Hacking" ; von der Planung über die Vertragsgestaltung zur Realisierung ; [mit Online-Service zum Buch], in: Edition Kes, 1. Aufl, Wiesbaden: Vieweg

Verzeichnis der Internet- und Intranet-Quellen

Book C. (2012)	Port-Scanning, http://rfc791.de/2012/07/11/port-scanning/, Abruf: 29.01.2014
Gartner (2007):	Gartner Identifies the Top 10 Strategic Technologies for 2008, http://www.gartner.com/it/page.jsp?id=530109, Abruf: 02.07.2010
Kendinibilir B. (2010):	IT-Sicherheit: Warum Unternehmen Penetrationstests durchführen sollten (und eigentlich auch müssen), http://blog.seibert-media.net/2010/11/03/it-sicherheit-warum-penetrationstests-durchfuehren/, Abruf: 04.01.2014
o.V (o.J.a):	Auslegung der GoB beim Einsatz neuer Organisations-technologien,http://www.awv-net.de/cms/Arbeitskreise /FA3_Wirtschaft_Recht/GoBS/AuslegungderGoBbeimEinsatzneuerOrganisationstechnologien,cat80.html, Abruf: 13.01.2014
o. V. (o. J. b):	TCP - Transmission Control Protocol, http://www.elektronik-kompendium.de/sites/net /0812271.htm, Abruf: 29.01.2014
o. V. (o. J. c):	Nmap,http://nmap.org/, Abruf: 20.01.2014
o. V. (o. J. d):	NAST Network Analizer Sniffer Tool, http://nast.berlios.de/#DESCRIPTION, Abruf: 07.01.2014
o. V. (o. J. e):	Knocker - The Net PortScanner, http://knocker.sourceforge.net, Abruf: 15.01.2014
o. V. (o. J. f):	Knocker - The Net Port Scanner - Screenshots, http://knocker.sourceforge.net/screenshots/knocker-gtk-0.6.6-E1.jpg, Abruf: 15.01.2014
o. V. (2013):	What is Angry IP Scanner ,http://angryip.org/w/Home, Abruf: 07.01.2014
o. V. (2014 a):	Übersicht über die aktuellen Cyberangriffe (aufgezeichnet von 180 Sensoren), Abruf: 18.01.2014

Galenski, S. (2002) Portscanner;http://ba-star.de/upload/1039100243 galenski_portscanner.pdf; Abruf: 30.01.14

o.V. (2014 b): Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (Zugangskontrolldiensteschutz-Gesetz - ZKDSG),http://www.buzer.de /gesetz/278/a3225.htm,
Abruf: 22.01.2014

Wagner F. (o.J.): Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG),http://wirtschaftslexikon. gabler.de/Definition/gesetz-zur-kontrolle-und-transparenz-im-unternehmensbereich-kontrag.html, Abruf: 15.01.2014

Wendehost T. (2013): Cyber-Angriffe live verfolgen,http://www. computerwoche.de/a/cyber-angriffe-live-verfolgen,2534329, Abruf: 17.01.2014

DHBW
Duale Hochschule
Baden-Württemberg
Stuttgart

Konzepte und Einsatzszenarien von Key-Value-Datenbanken

Schriftliche Ausarbeitung
im Rahmen der Lehrveranstaltung „Integrationsseminar“

Vorgelegt von

Bernd Graef,
Marc Sparn

am 24.01.2014

Fakultät Wirtschaft
Studiengang Wirtschaftsinformatik
WWI2011V

Inhaltsverzeichnis

Abkürzungsverzeichnis

BASE	Basically Available, Soft State, Eventual Consistency
CAP	Consistency, Availability, Partition Tolerance
MVCC	Multiversion Concurrency Control

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Im Rahmen der NoSQL-Bewegung sind in den letzten Jahren einige Datenbanken am Markt erschienen, die nicht auf relationaler Technologie basieren. Der Begriff NoSQL-Datenbanken ist ein Sammelbegriff für momentan ca. 150 verschiedene Systeme. [1]

NoSQL-Datenbanken gibt es in verschiedenen Ausprägungen. Eine dieser Ausprägungen sind die sogenannten Key-Value-Datenbanken, welche der zentrale Inhalt dieser Arbeit sind. Sie speichern Schlüssel-Wert-Paare und ermöglichen damit das schnelle Suchen über einen definierten Schlüssel.

Die Relevanz dieser Arbeit wird daran deutlich, dass das Thema NoSQL in den letzten Jahren immer populärer wurde und in dieser kurzen Zeit bereits Einzug bei teilweise sehr bekannten Firmen erhielt. Hintergrund ist dabei die problematische Handhabung extrem großer Datenmengen mit den marktführenden relationalen Datenbanken. Darauf wird im Verlauf dieser Ausarbeitung in Kapitel 2 vertieft eingegangen.

Ziel dieser Arbeit ist es, die grundlegenden Eigenschaften von NoSQL-Datenbanken darzustellen und einen Überblick über dieses Thema zu liefern. Ein zentraler Punkt ist dabei die Erstellung eines Kriterienkatalogs für Key-Value-Datenbanken. Dieser stellt die relevanten Aspekte anhand von sechs ausgewählten Anbietern dar und wird in Kapitel 3 näher beschrieben. Des Weiteren wird anhand eines Prototyps ein Vergleich einer Key-Value-Datenbank mit einer relationalen Realisierung durchgeführt. Dazu wird jeweils ein Vertreter der entsprechenden Gattung beispielhaft umgesetzt und eine Datenbank angelegt. Die Ergebnisse dieses Vergleichs werden in Kapitel 4 präsentiert.

Als Motivation zum Thema NoSQL- und Key-Value-Datenbanken wird im folgenden Abschnitt auf die Gründe der neuen Entwicklungen eingegangen. Zusätzlich soll eine Einführung in das Thema vorgenommen werden.

[1] Vgl. NoSQL-Database (o.J.)

2 Motivation und Einführung

Dieses Kapitel bietet eine Einführung in das Thema NoSQL-Datenbanken. Es untergliedert sich in die Geschichte der Datenbanken im Allgemeinen und die Grenzen relationaler Systeme im Zusammenhang mit Big Data. Abschließend wird das Thema NoSQL-Datenbanken genauer umrissen und eine Chronologie zur Entwicklung in den letzten Jahren aufgezeigt sowie eine Kategorisierung vorgenommen.

2.1 Geschichte der Datenbanken

Seit den 1970er Jahren haben relationale Datenbanken Einzug in den Unternehmen gehalten. Dies waren zunächst überwiegend kommerzielle Systeme (IBM, Oracle, …), auf welche mit der mächtigen Abfragesprache SQL zugegriffen werden konnte. [2]

In den 90er Jahren traten die objektorientierten Datenbanken in Erscheinung. Sie sollten den Entwicklern die mühsame Konvertierung der Datenobjekte in Reihen und Spalten ersparen. In der Praxis zeigten sich diese Systeme jedoch als sehr instabil, sodass nach weiteren Möglichkeiten gesucht wurde. In der Folge traten dann die sogenannten objektrelationalen Mapper (ORM) auf den Markt. [3]

Mit Beginn des 21. Jahrhunderts wurden die freien Implementierungen von relationalen Datenbanken immer beliebter. In diesem Zuge kamen Systeme wie MySQL, PostgreSQL und SQLite auf den Markt. Sie werden ebenfalls mit der Abfragesprache SQL bedient und sind in vielen Anwendungen im Einsatz. [4]

Durch den Einzug von Web 2.0 wuchsen die Datenmengen stetig und relationale Datenbanken stießen an ihre Grenzen, auf die in Kapitel 2.2 noch genauer eingegangen wird. Diese kommen insbesondere bei bekannten Internetunternehmen wie Google oder Facebook zum Tragen. Seit dem Jahr 2009 wurde damit einhergehend auch das Thema NoSQL-Datenbanken populär und bildet eine sinnvolle Alternative zu relationalen Datenbanken (s. Kapitel 2.3 NoSQL-Datenbanken).[5]

---

[2] Vgl. Schnelle, J. (2010)
[3] Vgl. Walker-Morgan, D. (2010)
[4] Vgl. Schnelle, J. (2010)
[5] Vgl. Edlich, S. u.a. (2010), S. 1

2.2 Big Data und Grenzen relationaler Systeme

Der Begriff Big Data ist zurzeit in aller Munde. Die Bedeutung des Begriffs definiert sich dabei über vier Eigenschaften: das Datenvolumen, die Vielzahl von Datenquellen, die Geschwindigkeit der Datenproduktion und -verarbeitungsowie die steigende Anzahl von Nutzern.

Problematisch dabei ist somit neben dem Datenvolumen, dass die Daten aufgrund vieler Datenquellen nicht einheitlich vorliegen. Zu den Erzeugern von Big Data zählen zusätzlich zu den mit Web 2.0 aufgetretenen Onlinedaten auch im Unternehmen produzierte Daten, z.B. im Bereich Gesundheitswesen oder Versicherungen. Die weltweite Datenmenge verdoppelt sich alle zwei Jahre und liegt laut einer Studie von Digital Universemomentan bei 1,8 Zettabyte. [6]Im Unternehmensumfeld entstehen diese Daten vor allem durch Logfiles, Sensoren, Transaktions- und Produktionsdaten. [7]

Die entstehenden großen Datenmengen stellen die Datenbanksysteme bezüglich der Speicherung und Auswertung vor große Probleme. Vor allem bei den Abfragen per SQL entstehen dadurch Performanceprobleme. Bei diesen Abfragen müssen bei jedem Suchvorgang alle Zeilen einer Tabelle durchsucht werden. Um dies zu vermeiden werden Indizes angelegt, die zusätzlichen Speicherplatz verbrauchen und einen weiteren Aufwand darstellen. Relationale Datenbanken sind aufgrund ihrer Architektur und Schemagebundenheit für häufige Transaktionen auf einzelnen Datensätzen ausgelegt. Ihre Einsatzstärken liegen bei einem kleinen bis mittleren Datenvolumen. Für den Umgang mit Datenmengen im Multi-Terabyte-Bereich sind sie unzureichend. Durch die vertikale Skalierung relationaler Datenbanksysteme entstehen im Zusammenhang mit Big Data somit hohe Kosten für die Aufrüstung der Systeme. Zudem ist vertikale Skalierung nur begrenzt möglich und damit stellen sich mit den wachsenden Datenmengen zunehmend Performanceverluste. [8]

2.3 NoSQL-Datenbanken

Der Begriff NoSQL-Datenbanken ist nicht exakt definiert, da es weder Gremien noch Organisation gibt, die sich mit einer Begriffsklärung beschäftigt haben. Das Verständnis des Begriffs variiert daher leicht, enthält im Kern jedoch stets die gleichen Elemente. [9]

---

[6] Vgl. Pientka, F. (2011)
[7] Vgl. Niemann, C. (2011)
[8] Vgl. ebenda
[9] Vgl. Edlich, S. u.a. (2010), S. 2

Auch bezüglich des Namens dieser Gattung von Datenbanken besteht eine angeregte Diskussion. Im Allgemeinen hat sich die Ansicht durchgesetzt, dass der Begriff als „Not Only SQL“ zu verstehen ist. Diese Annahme ergibt sich aus der Intention von NoSQL-Datenbanken, als Ergänzung zu den relationalen Systemen zu fungieren. Sie werden die relationalen Datenbanken nicht vollständig ablösen können, aber eine gute und wichtige Alternative im Zeitalter von Big Data (s. Kapitel 2.2 Big Data und Grenzen relationaler Systeme) bilden. [10]

Bevor die Kerneigenschaften genauer umrissen werden, wird zunächst auf die Entstehung des Begriffs anhand einer Chronologie eingegangen. Im Jahr 1998 wird der Begriff NoSQL erstmalig von Carlo Strozzi verwendet.[11] Sein Datenbankmodell stellte jedoch keine NoSQL-Datenbank nach der heutigen Ausprägung dar, sondern war lediglich ein relationales Datenbanksystem ohne SQL-API. Seit den 2000ern erhielt die NoSQL-Bewegung mit dem Einzug von Web 2.0 einen Aufschwung. Dafür war unter anderem Google mit dem sogenannten MapReduce-Ansatz (Kapitel 3.1.1) und dem BigTable-Datenbanksystem verantwortlich. Darüber hinaus legte Eric Brewer mit seiner Vermutung zum CAP-Theorem[12](Kapitel 3.1.2), welches 2002 durch Seth Gilbert und Nancy Lynch axiomatisch bewiesen wurden, einen weiteren Grundstein.[13] Im weiteren Verlauf zogen Firmen wie Yahoo, Amazon und verschiedene soziale Netzwerke nach. Viele der heute klassischen NoSQL-Systeme wie z.B. Redis und Riak, auf welche im weiteren Verlauf der Arbeit noch eingegangen wird, entstanden zwischen 2006 und 2009. Im Mai 2009 wurde der Begriff NoSQL in seinem heutigen Verständnis erstmals verwendet. Johan Oskarsson gebrauchte ihn bei einem Treffen zum Thema „Strukturierte, verteilte Datenspeicher“ in San Francisco. [14] Seitdem haben sich viele weitere Anbieter angeschlossen, sodass heute ca. 150 verschiedene NoSQL-Datenbanken existieren. [15]

Im NoSQL-Archivwird anhand verschiedener Kriterien versucht, eine Abgrenzung von NoSQL-Datenbanken zu relationalen Datenbanken vorzunehmen. Demnach versteht man unter dem Begriff eine neue Generation von Datenbanksystemen, welche einige der nachfolgenden Aspekte berücksichtigen:

1. Datenmodell ist nicht relational
2. Systeme sind auf eine verteilte und horizontale Skalierbarkeit ausgerichtet

[10] Vgl. Sadalage, P., Fowler, M. (2013), S. 11
[11] Vgl. Strozzi, C. (2010)
[12] Vgl. Brewer, E. (2000)
[13] Vgl. Gilbert, S., Lynch, N. (2002)
[14] Vgl. Edlich, S. u.a. (2010), S. 1f.
[15]Vgl. NoSQL-Database (o.J.)

3. Open Source
4. Schemafreiheit
5. Unterstützung von einfachen Datenreplikationen
6. Einfache API
7. Konsistenzmodelle sind EventuallyConsistent und BASE, aber nicht ACID

Wie der einleitende Satz bereits andeutet, decken die verschiedenen Systeme nicht alle dieser Punkte ab.[16]

Einige der genannten Begriffe werden im Folgenden noch erläutert. Für darüber hinaus gehende Information sei auf die angegebene Literatur verwiesen.

2.4 Kategorisierung von NoSQL-Datenbanken

Wie bereits angesprochen enthält das NoSQL-Archiv aktuell etwa 150 Systeme. Diese lassen sich im Kernbereich in vier Kategorien aufteilen. Darüber hinaus existieren noch einige nachgelagerte NoSQL-Systeme.Abb. 1 zeigt eine Abgrenzung relationaler Systeme zu NoSQL-Systemen und untergliedert letztere in Core NoSQL und Other NoSQL. [17]

Abb. 1: Relationale SQL-Systeme vs. NoSQL-Kategorien [18]

[16] Vgl. Edlich, S. u.a. (2010), S. 2
[17] Vgl. NoSQL-Database (o.J.)
[18] Enthalten in: Edlich, S. u.a. (2010), S. 6

Die vier in Abb. 1 dargestellten Kernsysteme bestehen aus Wide Column Stores, Document Stores, Key-Value-Stores und Graphdatenbanken. Den Hauptgegenstand dieser Arbeit bilden die Key-Value-Stores.

Key-Value-Systeme gelten als das einfachste der vier Kernmodelle. Bereits der Name verrät die Funktionsweise des Systems. Es stellt einen Schlüssel/Wert-Speicher dar, in dem jeder Schlüssel mit Werten verbunden ist. Über diese Schlüssel ermöglicht das System eine schnelle und effiziente Suche. Je nach System oder Anbieter können diese Schlüssel unterschiedliche Datentypen und Längen annehmen. Auch die Werte, die in den Datenbanken gespeichert werden variieren vom Typ und der Länge her je nach Anbieter. Key-Value-Stores lassen sich in zwei Untergruppen unterteilen. Zum einen die in-memory-Variante, welche die Daten im Arbeitsspeicher behält und somit eine hohe Performance aufweise, zum anderen die on-disk-Variante, welche die Daten direkt auf der Festplatte speichert.[19]

Abb. 2: Beispieleines Key-Value-Stores[20]

Abb. 2 zeigt die Beispiele einer Key-Value-Datenbank, Values in Sets, Listen oder Hashes abzulegen. Es wird deutlich, dass unter einem Key viele Values angesprochen werden können, die bei Hashes zudem mit Attributsnamen ergänzt werden.

[19] Redmond, E., Wilson, J. (2012), S. 4
[20] FH Köln (2013)

Auf einige ausgewählte Key-Value-Stores wird im Rahmen des Kriterienkataloges im folgenden Kapitel näher eingegangen. Dadurch wird nochmals eine tiefergehende Beschreibung von Key-Value-Stores vorgenommen

3 Kriterienkatalog

Nachdem im vorherigen Kapitel eine Einführung zum Thema NoSQL und Key-Value gegeben wurde, beschäftigt sich dieser Abschnitt mit einer Untersuchung verschiedener Key-Value-Stores nach ausgewählten Kriterien. Zunächst werden einige grundlegende Begriffe für das Verständnis des Katalogs geklärt. Anschließend wird eine Auswahl von geeigneten Key-Value-Systemen getroffen, welche abschließend untersucht und erläutert werden.

3.1 Grundlegende Begriffe zum Thema Key-Value

In den folgenden Unterkapiteln werden zentrale Konzepte zum Thema NoSQL behandelt. Dazu gehören das MapReduce-Verfahren, zusammenhängend mit dem CAP-Theorem das BASE-Konzept, das Prinzip des Konsistenten Hashings sowie die Multiversion Concurrency Control (MVCC).

3.1.1 MapReduce

Das MapReduce-Verfahren spielt eine entscheidende Rolle bei der Verarbeitung großer Datenmengen im TB-/PB-Bereich. Es ermöglicht eine effiziente nebenläufige Berechnung solcher Datenmengen. Das Framework wurde 2004 bei Google Inc. von den Entwicklern Jeffrey Dean und Sanjay Ghemawat entwickelt. Im Jahr 2010 erhielt Google das Patent für das MapReduce-Verfahren. [21]

Die Map-Funktion wird auf alle Datenelemente einer Liste angewendet und gibt eine modifizierte Liste zurück. Die Reduce-Funktion trägt die Ergebnisse einzelner Listenpaare zusammen und reduziert diese auf einen Ausgabewert. Durch den parallelen Ablauf beider Funktionen ist die Verarbeitung großer Datenmengen möglich. [22]

Das grundlegende Prinzip kann wie folgt verstanden werden: ein Problem wird in kleine Unterprobleme unterteilt, welche mit einem kleinen Anteil von Daten gelöst werden können.

[21] Vgl. Edlich, S. u.a. (2010), S. 12
[22] Vgl. Edlich, S. u.a. (2010), S. 13

Somit enthält der Speicher keine großen Datensätze. Zur Veranschaulichung befindet sich inAbb. 3 eine schematische Darstellung, die einen MapReduce-Prozess zeigt.

Abb. 3: Schematische Darstellung des MapReduce-Verfahrens [23]

3.1.2 CAP-Theorem und BASE

Das von Brewer geschaffene CAP-Theorem steht für Consistency, Availability und Partition Tolerance. Das Theorem besagt, dass ein verteiltes Datenbanksystem nur zwei dieser drei Punkte erfüllen kann. [24]

Die Consistency (Konsistenz) bedeutet dabei, dass alle Knoten zur selben Zeit dieselben Daten sehen können. In der Praxis bedeutet dies, dass erst nach der Aktualisierung aller Knoten ein Lesezugriff erfolgen kann. Die Availability (Verfügbarkeit) ist erreicht, wenn das System alle Anfragen beantwortet. Für einen konkreten Anwendungsfall muss daher eine akzeptable Reaktionszeit gegeben sein. Die Partition Tolerance (Ausfalltoleranz) ist gegeben, wenn der Ausfall eines Knoten des verteilten Systems aufgefangen werden kann und somit externe Anfragen weiterhin bearbeitet werden können.[25]

[23] Enthalten in: Edlich, S. u.a. (2010), S. 18
[24] Vgl. ebenda, S. 31
[25] Vgl. ebenda, S. 31f.

Abb. 4: CAP-Theorem[26]

Für die Lösung des Konflikts innerhalb des CAP-Theorems (s.Abb. 4) wird ein eigenes Konsistenzmodell für verteilte Datenbanksysteme verwendet. Dieses mit BASE (BasicallyAvailable, Soft-state, Eventual consistency) benannte Modell kommt bei vielen NoSQL-Datenbanken zum Einsatz und stellt das Gegenstück zum ACID-Prinzip relationaler Datenbanken dar. Der Hauptaspekt des BASE-Modells liegt in der Verfügbarkeit anstatt der Konsistenz. BASE verfolgt daher einen optimistischen Ansatz zur Konsistenz. Dies bedeutet, dass Systeme, welche nach BASE arbeiten, erst nach einem bestimmten Zeitfenster einen konsistenten Zustand erreichen und nicht unmittelbar nach einer Transaktion. Die garantierte Verfügbarkeit geht somit zu Lasten der durchgängigen Konsistenz. [27]

3.1.3 Konsistentes Hashing

Da bereits angesprochen wurde, dass es sich bei Key-Value-Datenbanken in der Regel um verteilte Systeme mit mehreren Knoten handelt, spielt das Hashing bei der gleichmäßigen Verteilung der Datenobjekte eine Rolle. Um Objekte einem festen Speicherort zuzuweisen, werden Hashfunktionen verwendet, welche die Objekte z.B. auf feste Server verteilen. Eine

[26] Enthalten in: Smith, S. (2012)

[27] Vgl. ebenda, S. 33f.

wichtige Aufgabe der Hashfunktion ist dabei die gleichmäßige Verteilung von Ergebnissen auf die verschiedenen Knoten des verteilten Systems. [28]

Das konsistente Hashing, im Original von Karger, D. (u.a.) veröffentlicht[29], setzt verschiedene Anforderungen um. Zum einen soll beim Hinzufügen eines neuen Servers in das bestehende verteilte System ein möglichst geringer Anteil der gespeicherten Daten neu verteilt werden. Zum anderen sollen beim Wegfall eines Servers lediglich die dort enthaltenen Daten auf die verbleibenden Knoten umverteilt werden. Bei der Verteilung der Daten über die verschiedenen Server wird anstatt der gleichmäßigen Verteilung die individuelle Speicherkapazität der Server betrachtet.[30]

Abb. 5: Abbildung von Servern und Objekten auf einen Ring[31]

Das konsistente Hashing lässt sich anhand der kreisförmigen Darstellung in Abb. 5 besser erläutern. Zunächst werden die Server nach ihren Hashwerten in den Adressraum eingefügt. Anschließend wird den Objekten ein Platz im Adressraum zugewiesen, der sich ebenfalls aus deren Hashwert ergibt. Das Objekt wird auf dem im Uhrzeigersinn nächstgelegenen Server abgelegt. Falls ein neuer Server hinzukommt, übernimmt dieser alle Objekte zwischen dem Hashwert seines Vorgängers und seinem eigenen. Wird ein Server aus dem verteilten System entfernt, übernimmt dessen Nachfolger all seine Objekte. Zur ausgeglichenen Lastverteilung wird den Servern je nach Leistungsfähigkeit eine entsprechende Anzahl von Hashwerten zugeordnet. [32]

[28] Vgl. Edlich, S. u.a. (2010), S. 37
[29] Vgl. Karger, D. u.a. (1997)
[30] Vgl. ebenda, S. 37
[31] Enhalten in: Edlich, S. u.a., S. 38
[32] Vgl. Edlich, S. u.a., S. 38f.

3.1.4 Multiversion Concurrency Control

Die Multiversion Concurrency Control befasst sich mit der korrekten Speicherung aller Datensätze sowie deren semantischer Integrität. Einhergehend mit dem Auftreten von Web 2.0 und den veränderten Anforderungen an moderne Datenbankanwendungen, wird eine Alternative zu den klassischen Sperrverfahren bei Lese- und Schreibvorgängen benötigt. Als Lösung hierfür gibt es bei der MVCC keine Sperren mehr bei Datenzugriffen. Stattdessen werden mehrere unveränderliche Versionen der Datensätze in einer zeitlichen Reihenfolge gehalten. Bei aktiven Schreibvorgängen können parallele Lesezugriffe auf frühere Versionen der jeweiligen Datensätze durchgeführt werden. Zur Verhinderung von Schreibkonflikten wird die angegebene Vorgängerversion mit der aktuellen Vorgängerversion verglichen. Dadurch entstehende Widersprüche werden über ein Rollback oder Neustart der Transaktion gehandhabt. Durch das Halten der verschiedenen Versionen von Datensätzen, wird für das MVCC-Konzept mehr Speicherplatz und Rechenzeit benötigt. Nicht mehr verwendete Versionen werden aus dem System gelöscht. Diese Aspekte machen das MVCC-Konzept zu einem interessanten AnsatzfürNoSQL-Systeme, der aber auch in relationalen Datenbanken zum Einsatz kommt. MVCC ist in verschiedenen Implementierungen mit unterschiedlicher Transparenz des Systems vorhanden und hat damit einhergehend auch verschiedene Verfahren zur Konfliktbehandlung.[33]

3.2 Auswahl geeigneter Key-Value-Stores

Für die Auswahl der für einen Kriterienkatalog geeigneten Key-Value-Stores wurde zunächst eine Grobauswahl anhand der Liste auf http://nosql-database.org vorgenommen. Basierend auf dem jeweiligen Informationsangebot der Homepages der einzelnen Datenbanken konnte eine genauere Eingrenzung durchgeführt werden. Auch die in der Aufgabenstellung genannten Vertreter für Key-Value-Datenbanken wurden für die Entscheidung genauer betrachtet. Ein wichtiger Aspekt für die endgültige Auswahl war das DB-Engines Ranking zu Key-Value-Stores (s. Abb. 6). In Anbetracht des zeitlichen Limits wurde eine Anzahl von sechs Datenbanken festgelegt. Die Wahl folgte auf die laut DB-Engines sechs beliebtesten Vertreter im Bereich der Key-Value-Stores: Redis, Memcached, Riak, Ehcache, DynamoDB und BerkeleyDB.

[33] Vgl. ebenda, S.42ff.

39 Systeme im Ranking, Januar 2014

Rang	Vormonat	DBMS	Datenbankmodell	Punkte	Änderung
1.	1.	Redis	Key-Value Store	52,49	+0,72
2.	2.	Memcached	Key-Value Store	35,98	-0,11
3.	3.	Riak	Key-Value Store	10,46	+0,24
4.	4.	Ehcache	Key-Value Store	8,20	-0,37
5.	5.	DynamoDB	Key-Value Store	7,52	+0,09
6.	6.	Berkeley DB	Key-Value Store	3,84	-0,80
7.	7.	SimpleDB	Key-Value Store	3,55	+0,13
8.	8.	Hazelcast	Key-Value Store	3,01	+0,27
9.	9.	Coherence	Key-Value Store	2,96	+0,27
10.	10.	Oracle NoSQL	Key-Value Store	1,45	+0,05

Abb. 6: DB-Engines Ranking[34]

Dieses Ranking stellt eine Rangliste von Datenbankmanagementsystemen dar und wird monatlich aktualisiert. Gemessen wird dies anhand der Anzahl der Nennungen des Systems auf Websites, dem allgemeinen Interesse an dem System, der Häufigkeit technischer Diskussionen über das System, der Anzahl an mit dem System zusammenhängenden Job-Angeboten und der Anzahl an Profilen in professionellen Netzwerken, in denen das System aufgeführt wird.[35]

3.3 Untersuchung der ausgewählten Systeme

Dieses Kapitel betrachtet die in Kapitel 3.2 ausgewählten Key-Value-Stores im Rahmen eines Kriterienkataloges. Im Folgenden werden die genannten sechs Systeme nach verschiedenen Kategorien und Einzelaspekten beschrieben. Als Oberkategorien wurden Basisinformationen zur Datenbank, Eigenschaften der Datenbank, das verwendete Modell, die möglichen Schnittstellen und Utilities ermittelt.

3.3.1 Basisinformationen

Der erste zu betrachtende Block mit den Basisinformationen zu den Datenbanken enthält Informationen zum Anbieter, zu den Versionen, zum Lizenzmodell, zu unterstützten Plattformen und zur Entwicklungssprache. Zudem wird eine Charakterisierung der Datenbank vorgenommen. Der Unterpunkt „Webseite“ enthält die jeweilige Homepage des Anbieters und

[34] Enthalten in: Solid IT (2014 a)
[35] Solid IT (2014 b)

führt zu detaillierten Informationen zu den verschiedenen Systemen. Die „Erste Version“ bezeichnet das erste marktfähige Release des Projekts.

Datenbank			Redis	Berkeley DB	Memcached
Basis					
	Anbieter		Open Source Projekt	Oracle	Danga Interactive
	Webseite		Redis.io	http://www.oracle.com/us/products/database/berkeley-db/overview/index.html	http://memcached.org/
	Erste Version		2009	1994	2003
	Untersuchte Version		2.8.2	6.0.20	1.4.15
	Lizenz Open Source		BSD-Lizenz	GNU APGL v3.0	BSD-Lizenz
	Lizenz Kommerziell		nein	ja, duales Lizenzmodell	nein
	Plattform				
		Windows	nein	ja	ja
		Linux	ja	ja	ja
		Unix	ja	ja	ja
		MacOS	ja	ja	ja
		Andere	OpenBSD, FreeBSD, Solaris	AIX, Sun Solaris, SCO Unix	Unix-Derivate
	Eigene Charakterisierung		Caches, die Web- oder Sitzungsdaten speichern	Eingebettetes Datenbanksystem	Cache-Server
	Entwickelt in		C / C++	C	C

Tabelle 1: Basisinformationen zu Redis, BerkeleyDB und Memcached

Tabelle 1 zeigt die Basisinformationen zu den drei Systemen Redis, BerkeleyDB und Memcached. Die ersten Unterschiede zeigen sich bei den Anbietern der Systeme. Während Redis ein Community Projekt ist, sind BerkeleyDB und Memcached von Firmen entwickelte Datenbanken. Bezüglich des Lizenzmodells unterscheidet sich die BerkeleyDB dahingehend, dass sie ein duales Lizenzmodell besitzt, während Redis und Memcached nur eine kostenlose BSD-Lizenz haben. Die duale Lizenz der BerkeleyDB gliedert sich in eine Public License und eine Closed Source License. Für die kostenlose Public License gilt, dass die Software, unter der die BerkeleyDB genutzt wird, Open Source ist. Bei Software, die nicht Open Source ist, wird die kostenpflichtige Closed Source License benötigt. Auffällig ist, dass Redis Windows nicht unterstützt. Eine Anwendung unter Windows ist durch einen Windows Port möglich, der von der Microsoft Open Tech Group zur Verfügung gestellt wird.[36]

[36]http://github.com/MSOpenTech/redis

Datenbank			DynamoDB	riak	ehcache
Basis					
	Anbieter		Amazon	Basho Technologies	terracotta
	Webseite		http://aws.amazon.com/de/dynamodb/	http://docs.basho.com/	ehcache.org
	Erste Version		18.01.2012	17.08.2009	13.11.2003
	Untersuchte Version		31.10.2013	1.4 (10.07.2013)	2.7.0 (04.03.2013)
	Lizenz Open Source		kostenloses Kontingent	Apache 2.0	Apache 2.0
	Lizenz Kommerziell		Zahlung nach Stundensätzen, Vertrag	kostenpflichtige Enterprise Version	in Big Memory Max enthalten
	Plattform		Plattformunabhänig, gehostet		Plattformübergreifend
		Windows	ja	nein	ja
		Linux	ja	ja	ja
		Unix	ja	nein	ja
		MacOS	ja	ja	ja
		Andere	ja	BSD, Solaris	ja
	Eigene Charakterisierung		vollständig verwaltet	fehlertolerante open-source DB	freie Software für die Umsetzung von Caches in Java Programmen
	Entwickelt in		keine Angaben	Erlang, C, C++, etwas Java-script	Java

Tabelle 2: Basisinformationen zu DynamoDB, Riak und Ehcache

Tabelle 2 bezieht sich nun auf die Basisinformationen zu der DynamoDB, Riak und Ehcache. Erwähnenswert sind hierbei die unterschiedlichen Lizenzmodelle der drei Anbieter. Während Riak und Ehcache eine kostenlose Apache 2.0-Lizenz anbieten, stellt Amazon für die DynamoDB lediglich ein kostenloses Kontingent zur Verfügung, welches bei Überschreiten über Stundensätze vertraglich abgerechnet wird. Das kostenlose Kontingent beinhaltet für Privatpersonen 100 MB Speicher, 5 Schreib- und 10 Lesekapazitätseinheiten pro Sekunde für ein Jahr. Für die kommerzielle Version können im Voraus zudem Abonnements über reservierte Kapazitäten geschlossen werden. Auch Riak und Ehcache bieten kommerzielle Lizenzmodelle an. Die kostenpflichtige Riak-Version bietet im Vergleich zum Open-Source-Produkt zusätzliche Features an. Wie bereits bei Redis gesehen, unterstützt auch Riak die Anwendung unter Windows nicht. Ebenso wird hier Unix nicht unterstützt, wohingegen die anderen Anbieter plattformunabhängig sind. Ein besonderes Merkmal der DynamoDBist, dass die Verwaltung der benötigten Ressourcen vollständig in Form eines Services von Amazon bewältigt wird.

Passend zu den Basisinformationen zeigt Abb. 7 einen Verlauf der Beliebtheit der behandelten Datenbanksysteme im DB-Engines Ranking über die letzten 14 Monate. Redis und Memcached zeigen sich hierbei mit großem Abstand als die beiden führenden Vertreter der Key-Value-Stores in diesem Ranking.

Abb. 7: Verlauf des DB-Engines Ranking[37]

3.3.2 Datenbankeigenschaften

Der zweite Abschnitt des Kriterienkatalogs befasst sich mit den jeweiligen Datenbankeigenschaften. Dazu zählen neben den klassischen Datenbankeigenschaften auch NoSQL-spezifische Eigenschaften.

Datenbank		Redis	Berkeley DB	Memcached
DB-Eigenschaften				
	Replikation	Master/Slave-Replikation	Master/Slave-Replikation, Paxos bei Master-Wahl	keine, nur per Patch (Repcached) möglich
	Transaktionen	nein	ja, ACID	nein
	Persistenz (Storage Engine)	Snapshot / Append Only File	ja	nein
	In-Memory	ja	ja	ja
	On-Disk	ja	ja	nein
	Embeddable	nein	ja	ja
	Versionen	nein		nein
	Verteilung	Horizontal skalierbar	Horizonal skalierbar	Sharding
	Indizierung	kein Sekundärindex	kein Sekundärindex	kein Sekundärindex
	Sicherheit	Passwörter	kein Berechtigungskonzept	SASL-Protokoll
	Mehrbenutzerkonzept	Lock-Free Model, Optimistic Locking, Datenzugriffe werden	MVCC	Lock-Free Modell
	Load Balancing	Consistent Hashing	nein	Hashing, Consistent Hashing
	MapReduce	nein	nein	nein
	Volltextsuche	nein	ja	nein
	Sonstiges			

Tabelle 3: Datenbankeigenschaften zu Redis, BerkeleyDB und Memcached

[37] Enthalten in: Solid IT (2014c)

Der in Tabelle 3 gezeigte Ausschnitt des Kriterienkataloges enthält die Datenbankeigenschaften zu Redis, BerkeleyDB und Memcached. Redis und BerkeleyDB verfügen über die Möglichkeit der Master/Slave-Replikation, während Memcached standardmäßig keine Replikation zur Verfügung stellt. Diese Funktion kann über einen Patch hinzugefügt werden. Die Speicherung ist bei Redis und BerkeleyDB sowohl im Arbeitsspeicher und auf der Festplatte möglich, bei Memcached ausschließlich im Arbeitsspeicher. Auffällig ist, dass BerkeleyDB kein spezielles Berechtigungskonzept verwendet. Das in Kapitel 3.1.3 beschriebene konsistente Hashing wird von Redis und Memcached unterstützt, von derBerkeleyDB jedoch nicht. Eine Besonderheit der BerkeleyDB ist die Möglichkeit einer Volltextsuche sowie die Verwendung des für relationale Datenbanken typischen ACID-Konzepts.

Datenbank	DynamoDB	riak	ehcache
DB-Eigenschaften			
Replikation	multiple availability zones, master-slave	Peer-basiert, Master/Master	symmetrische Replikation über RMI, Jgroup, JMS
Transaktionen	nein	nein	Java Transaktions API, ACID
Persistenz (Storage Engine)	ja	Dauerhaftes Schreibquorum	verschiedene Persistenzoptionen
In-Memory	nein	ja	ja
On-Disk	ja, SSD	ja	ja
Embeddable	nein (gehostet)	nein	einfach in bestehende Java-Applikationen
Versionen	ja, optimistic locking support	ja, vector clock	nein
Verteilung	horizontale skalierung, sharding	Rechenzentrum, sharding	horizontale Skalierung
Indizierung	Sekundärindex (über range type keys)	Sekundärindex	Sekundärindex
Sicherheit	Verschlüsselung, Passwort	keine	standardmäsig keine konfiguriert
Mehrbenutzerkonzept	eventually consistent	MVCC	explicit locking (read und write)
Load Balancing		Ja, consistent hashing	ja, über Automatic Resource Control (ARC)
MapReduce	ja (über Amazon EMR)	ja	ja
Volltextsuche	nein	ja	nein
Sonstiges	Architektur: shared-nothing	Architektur: shared-nothing	

Tabelle 4: Datenbankeigenschaften zu DynamoDB, Riak und Ehcache

Tabelle 4 beinhaltet die Datenbankeigenschaften zu DynamoDB, Riak und Ehcache. Diese unterscheiden sich im Bereich der Transaktionen dahingehend, dass nur Ehcache diese ermöglicht. Im Gegensatz zu Riak und Ehcache kann DynamoDB lediglich auf der Festplatte speichern. Ehcache ist eine javaspezifische Datenbank und bietet daher auch eine einfache Einbindung in bestehende Java-Applikationen. Im Gegensatz zur Open-Source-Version von Ehcache bietet die Enterprise Edition verschiedene Sicherheitskonzepte, welche SSL-, LDAP- oder JMX-basiert sind, an. Die Sicherheit bei DynamoDB wird über Kryptographiemethoden geregelt, welche vom AWS Identity and Access Management bereitgestellt werden. Im Vergleich zu den Anbietern aus Tabelle 3 ermöglichen alle drei Anbieter die Suche über

einen Sekundärindex und das MapReduce-Verfahren. Wie auch die BerkeleyDB wird bei Ehcache das ACID-Konzept eingesetzt.

3.3.3 Datenbankmodell

Der nächste Block des Kriterienkataloges bezieht sich auf die Datenbankmodelle der sechs Systeme. Betrachtet werden hierbei die möglichen Datentypen für die Keys und Values, welche in Tabelle 5 und Tabelle 6 dargestellt werden. Unter einfachen Datentypen werden im Folgenden Integer, Boolean und Strings zusammengefasst.

Datenbank	Redis	Berkeley DB	Memcached
Modell			
Key	Binary Safe Strings, max 2^31 Bytes	byte strings feste / variable länge, max 2^32 Bytes	Beliebiger String, maximale Länge 250 Bytes
Value		byte strings feste oder variable länge	32 Bit Flag Value, 64 Bit CAS Value (unique)
Einfache Typen	ja	ja	ja
Liste	ja		
Menge	ja		
Hashes	ja	ja	
Sonstiges	geordnete Mengen möglich		

Tabelle 5: Datenbankmodell zu Redis, BerkeleyDB und Memcached

Der grundlegende Datentyp für den Key ist bei allen drei Datenbanksystem ein String. Gravierende Unterschiede bestehen jedoch bei der maximalen Länge der Keys. Die Binary Safe Funktion behandelt ihren Inhalt als rohen Datenstrom ohne Format. Im Fall von Redis bedeutet dies, dass der Key jegliche Arten von Daten enthalten kann, z.B. auch JPEG-Bilder. Während bei Redis und BerkeleyDB 2^31 bzw. 2^32 Bytes möglich sind, erlaubt Memcached lediglich eine Länge von 250 Bytes. Bezüglich der Datentypen für die Values ist Redis am flexibelsten. Hier werden neben allen Standardtypen auch geordnete Mengen unterstützt. Strings werden bei Redis bis zu 512 MB unterstützt. Für Listen, Mengen und Hashes gilt eine maximale Größe von 2^32-1 Elementen.

Datenbank			DynamoDB	riak	ehcache
Modell					
	Key		Hash Type (2048 Bytes), Hash and Range Type (1024 Bytes)	binär, string, max 255 Bytes (bei innostore)	alle Standarddatentypen
	Value		bis 64 KB		alle Standarddatentypen
		Einfache Typen	ja	ja	ja
		Liste	ja	ja	ja
		Menge	ja	ja	ja
		Hashes			ja
	Sonstiges			JSON, XML, Images, Video-Clips	

Tabelle 6: Datenbankmodell zu DynamoDB, Riak und Ehcache

Die in Tabelle 6 dargestellten Systeme unterscheiden sich bezogen auf den Key in erster Linie von den in Tabelle 5 behandelten Systemen. Hier werden neben Strings auch andere Datentypen wie beispielsweise der Hash Type bei DynamoDB unterstützt. Die maximale Länge der Keys reicht hier jedoch nur von 255 Bytes bis maximal 2048 Bytes. Hervorzuheben ist, dass Ehcache bezüglich der Keys und Values alle Standarddatentypen unterstützt. Auch Riak bietet eine Besonderheit, indem es Formate wie JSON, XML, Images und Videos als Value unterstützt. Die Speicherung der Daten bei Riak erfolgt in Form von Objekten, welche sich aus sogenannten Buckets, Keys, VectorClocks[38] und einer Liste von Metadaten zusammensetzen.

3.3.4 Schnittstellen

Der folgende Abschnitt beschäftigt sich mit den Schnittstellen der untersuchten Datenbanksysteme. Damit einhergehend werden sowohl die APIs als auch die Protokolle der jeweiligen Systeme untersucht.

Datenbank			Redis	Berkeley DB	Memcached
Schnittstelle					
	APIs				
		Java	ja	ja	ja
		C#	ja	ja	nein
		C++	ja	ja	ja
		Andere	PHP, Ruby, Python, Perl, Lua, Erlang, Scala, C, TCL, JavaScript, uvm.	Perl, Python, uvm.	C, PHP, Perl, Python, Ruby, ASP.NET
	Protokolle				
		HTTP	nein	nein	nein
		REST	nein	nein	nein
		Sonstige	Über die Programmiersprache	Über die Programmiersprache	Memcached-Protokoll

Tabelle 7: Schnittstellen von Redis, BerkeleyDB und Memcached

[38] docs.basho.com/riak/latest/theory/concepts/Vector-Clocks/

Tabelle 7 zeigt, dass die Standardsprache Java, C# und C++ gewöhnlich unterstützt werden. Lediglich Memcached hat keine C#-API. Der Zugriff über HTTP- und REST-Protokolle ist bei den drei Anbietern nicht möglich und erfolgt stattdessen über die Programmiersprache bzw. im Falle von Memcached über ein spezielles Protokoll.

Datenbank			DynamoDB	riak	ehcache
Schnittstelle					
	APIs				
		Java	ja	ja	ja
		C#	nein	nein	ja
		C++	nein	ja	ja
		Andere	android, ios, .NET, Node.js, Python, PHP, Ruby	Python, PHP, Node.js, Ruby, Erlang, c, Rest	c, PHP, Python, Ruby
	Protokolle				
		HTTP	ja	ja	ja
		REST	ja	ja	ja
		Sonstige			SOAP

Tabelle 8: Schnittstellen von DynamoDB, Riak und Ehcache

Bezogen auf die Standardsprache wird in Tabelle 8 gezeigt, dass DynamoDB lediglich den Zugriff über Java ermöglicht. Riak besitzt keine C#-Schnittstelle und Ehcache deckt alle drei Standardsprachen ab. Auffällig ist, dass alle Systeme aus den Tabellen 7 und 8 eine Schnittstelle zu Java besitzen. Darüber hinaus ist bei allen sechs Systemen der Zugriff über viele weitere APIs, inbesondere Python und Ruby, möglich. Während in Tabelle 7 keine Unterstützung von HTTP und REST gegeben war, bieten alle Systeme in Tabelle 8 diese Protokolle an.

3.3.5 Utilities

Der letzte große Block des Kriterienkataloges sind die Utilities. Dieser Bereich betrachtet verschiedene Werkzeuge, die unter anderem die Administration sowie den Import und Export unterstützen.

Datenbank		Redis	Berkeley DB	Memcached
Utilities				
	Shell	Redis.cli		Command Line
	Adminwerkzeug	Redis Configuration File (redis.conf)		telnet, memcached-top, stats-proxy, memcache.php, PhpMemcacheAdmin, Memcache Manager
	IDE Integration	Jedis und JRedis für Java	Bibliotheken zum Einbinden	Eclipse
	Import	Redis Protocol Format		
	Export			
	Ladewerkzeug	netcat Pipe Mode		Brutis, Memcachetest, Memslap, mc-loader

Tabelle 9: Utilities von Redis, BerkeleyDB und Memcached

Aus Tabelle 9 ist ersichtlich, dass zur BerkeleyDB wenige Utilities gefunden wurden. Speziell im Bereich der Adminwerkzeuge wurde bei Memcached eine ganze Reihe von Tools ausfindig gemacht, die den User des Systems bei den administrativen Aufgaben unterstützen sollen. Die Einbindung der Systeme in Entwicklungsumgebungen erfolgt zumeist über verfügbare Bibliotheken.

Datenbank		DynamoDB	riak	ehcache
Utilities				
	Shell	dynach	mingfai	
	Adminwerkzeug	AWS	riak control	Terracotta Management Console (TCM)
	IDE Integration	Eclipse, Visual Studio		Eclipse
	Import	AWS Data pipeline	riak-data-migrator	
	Export	AWS Data pipeline	riak-data-migrator	
	Ladewerkzeug	AWS Data pipeline	riak-data-migrator	
	Sonstiges			Einbindung in Spring, Hibernate

Tabelle 10: Utilities von DynamoDB, Riak und Ehcache

Die Anbieter von DynamoDB, Riak und Ehcache liefern für ihre Systeme auch Adminwerkzeuge wie in Tabelle 10 ersichtlich ist. Für DynamoDB und Riak gibt es jeweils umfassende Tools, welche den Im- und Export ermöglichen sowie als Ladewerkzeug fungieren.

3.4 Erkenntnisse des Kriterienkataloges

Die Erkenntnisse der Kategorie Basis zeigen, dass es sich bei den untersuchten Systemen um vorwiegend junge Produkte handelt. Dies ist dem Aspekt geschuldet, dass es sich bei der NoSQL-Bewegung um eine relativ neue Bewegung handelt. Dennoch weisen die untersuchten Systeme unterschiedliche Reifegrade auf. Entsprechend der Intention von NoSQL

sind die Lizenzmodelle in der Regel Open Source, mit teilweise kommerziellen Add-Ons. Die Entwicklungssprache für die sechs Anbieter ist überwiegend C.

Zu den Datenbank-Eigenschaften ist abschließend zu sagen, dass zumeist die Möglichkeit der Replikation angeboten wird. Bezüglich der Persistenz werden verschiedene Modelle mit Kombinationen aus In-Memory- bzw. On-Disk-Varianten eingesetzt. Generell wird im Gegensatz zu relationalen Daten auf das CAP-Theorem und den BASE-Ansatz aufgesetzt. Darüber hinaus finden auch weitere NoSQL-typische Techniken wie MapReduce, MVCC und ConsistentHashing Berücksichtigung.

Das Modell der Datenbank liefert Erkenntnisse zu den unterstützten Datentypen und maximalen Längen bei Keys und Values. Auffällig ist der hohe Anklang von Strings bei den Keys, welche bezüglich der Länge großen Schwankungen von 250 Bytes bis zu 2^32 Bytes unterliegen. Für die Values stehen in der Regel alle Standarddatentypen zur Verfügung. Je nach Anbieter besteht zudem die Möglichkeit Listen, Mengen, Hashes oder ganze Dateien zu nutzen.

Der Bereich Schnittstelle stellt Java als konstante API für alle sechs Systeme heraus. Zudem finden Ruby, Python, C#, C++ und PHP häufig Unterstützung. Als Protokolle kommen gleichermaßen HTTP / REST oder programmiersprachenbasierte Protokolle zum Einsatz. Allgemein bieten alle sechs Systeme Support durch Werkzeuge an, welche zumeist vom Anbieter des Systems zur Verfügung gestellt werden.

4 Prototypischer Vergleich eines Key-Value-Stores mit einer relationalen Realisierung

Dieses Kapitel beschäftigt sich mit einem prototypischen Vergleich zwischen einem Key-Value-Store und einer relationalen Realisierung einer Datenbank. In Kapitel 4.1 Aufbau des Prototyps wird erläutert, welches Anwendungsszenario für den Vergleich ausgewählt wurde und darauf basierend die Wahl des geeigneten Key-Value-Stores getroffen. Der Abschnitt 4.2 Vergleich Key-Value-Store mit relationalem System beschreibt Unterschiede und Ergebnisse, die sich beim Vergleich mit Hilfe des Prototyps herauskristallisiert haben.

4.1 Aufbau des Prototyps

Für den prototypischen Vergleich wird ein bestimmtes Anwendungsszenario zugrunde gelegt. In dieser Arbeit wurde sich für ein Onlineforum entschieden. In diesem Forum melden sich verschiedene Benutzer mit ihren persönlichen Daten an. Dies sind eine eindeutige, automatisch zugewiesene User-ID, ein Username, ein Passwort, die Adresse bestehend aus Postleitzahl, Stadt und Straße, der Name, der Vorname sowie das Geburtsdatum. Angemeldete Benutzer können in diesem Forum Beiträge verfassen, private Nachrichten verschicken und auf sämtliche Bereiche des Forums zugreifen. Weitere potenzielle Einsatzmöglichkeiten stellen sämtliche Arten sozialer Netzwerke sowie der Online Warenkorb verschiedener Versandhäuser dar.

Für die Realisierung des Prototyps wurde das Datenbanksystem Redis gewählt. Die Auswahl dieses Systems aus den sechs im Kriterienkatalog (Kapitel 3.3) wurde unter anderem aufgrund des Lizenzmodells getroffen. Weiterhin hat die Unabhängigkeit von Redis bezüglich der Datentypen der Values zur Entscheidung beigetragen. Darüber hinaus hat Redis Performancevorteile bei Web- und Sitzungsdaten, insbesondere, wenn diese vom Umfang her in den Arbeitsspeicher passen. Zudem besteht auf der Webseite eine sehr ausführliche Dokumentation, welche eine Einführung in die Anwendung dieses Systems detailliert beschreibt. Die relationale Umsetzung des Forums wurde mit einer MySQL-Datenbank realisiert.

Für die Key-Value-basierte Implementierung des Anwendungsszenarios wurde zunächst der Windows Port der Open Tech Group (Kapitel 3.3) installiert. Nach der Ausführung mit Microsoft Visual Studio, standen der Redis Server sowie die wichtigen Werkzeuge zur Verfügung. Anschließend wurde die Redis-Bibliothek „Jedis“ in die Entwicklungsumgebung Eclipse integriert, damit eine Java-Lösung umgesetzt werden konnte. Darauf basierend konnte mit dem Aufbau des Prototyps mit Hilfe von Java begonnen werden.

Zunächst wird eine Verbindung der Datenbank mit dem Redis Server hergestellt. Für den Prototyp wurden 15 Beispieluser mit den bereits genannten Attributen angelegt. Dabei wurde die User_ID als Key verwendet, da sie jeden User eindeutig identifiziert. Die weiteren Attribute wurden mittels eines Hashtypes angelegt. Abb. 8 zeigt beispielhaft die Anlage eines Users anhand des verwendeten Codes. Die Methode aus der Jedis-Bibliothek zur Anlage eines Hashtypes lautet HSet(key, field, value).

```
jedis.hset("user7", "username", "leni");
jedis.hset("user7", "passwort", "möhre");
jedis.hset("user7", "plz", "40213");
jedis.hset("user7", "stadt", "Düsseldorf");
jedis.hset("user7", "strasse", "Parkstraße");
jedis.hset("user7", "name", "Brandt");
jedis.hset("user7", "vorname", "Lena");
jedis.hset("user7", "geburtsdatum", "05.11.1946");
```

Abb. 8: Screenshot Anlage eines Users in Redis

Oben stehendes Beispiel nutzt den Key „user7“, Fields sind die weiteren Attribute der Datenbank, die Values sind die jeweiligen Ausprägungen der Attribute für den entsprechenden User. Nach diesem Schema wurden alle 15 User angelegt. Redis liefert zwei Möglichkeiten zur Abfrage der Datensätze. Einerseits kann mit der Methode HGetAll(Key) der gesamte Inhalt des Hashtypes eines Keys abgefragt werden. Andererseits bietet die Methode HGet(Key, Field) die Abfrage des Values zu einem bestimmten Field des Keys an.

Für die relationale Umsetzung mit MySQL wurde eine Datenbank „forum“ mit fünf normalisierten Tabellen erstellt, die in Abb. 9 zu sehen sind. Zusätzlich zu der Normalisierung wurde im Sinne des Sicherheitsgedanken die Speicherung des Passwortes in eine separate Tabelle vorgenommen. Die Tabelle User wurde von der Tabelle Daten getrennt, da es sich beim Usernamen um keine persönlichen Daten im engen Sinn handelt. Die Abfrage erfolgt per SQL Statement aus einer Java-Klasse heraus.

Abb. 9: Tabellen der relationalen Datenbank

Nachdem nun der Aufbau des Prototyps abgeschlossen ist, wird im folgenden Abschnitt der Vergleich der beiden Implementierungen vorgenommen.

4.2 Vergleich Key-Value-Store mit relationalem System

Der Vergleich des Key-Value-Stores mit dem relationalen System wurde wie die Implementierung in Kapitel 4.1 mit Java vorgenommen. Für den Vergleich wurden für beide Varianten Datenbankabfragen eingesetzt, die jeweils alle Attribute eines bestimmten Users anzeigen sollen. Sie werden in Abb. 10und Abb. 11dargestellt.

```
Map<String, String> value = jedis.hgetAll("user1");
```

Abb. 10: Datenbankabfrage in Redis

Die Abfrage der Redis-Datenbank beläuft sich auf eine Codezeile. Über die bereits angesprochene Methode HGetAll(Key) (Kapitel 4.1) werden im Beispiel aus Abb. 11die Attribute zu User1 abgefragt. Die Ergebnisse werden im Attribut „value“ als Map<String, String>-Datentyp gespeichert.

```
String SQLString = "SELECT user.USER_ID, user.username, passwort.pw, plz.plz, plz.stadt, " +
                    "adresse.strasse, daten.name, daten.vorname, daten.geburtsdatum " +
                    "FROM user " +
                    "JOIN passwort ON user.USER_ID = passwort.USER_ID " +
                    "JOIN adresse ON user.USER_ID = adresse.USER_ID " +
                    "JOIN daten ON user.USER_ID = daten.USER_ID " +
                    "JOIN plz on plz.PLZ = (select plz from adresse where user_id = 5) " +
                    "WHERE user.USER_ID =5;";
```

Abb. 11: Datenbankabfrage in SQL

Im Vergleich zur Abfrage auf die Redis-Datenbank ist der Umfang der relationalen Datenbankabfrage deutlich größer. Mittels eines SQL-Statements werden auch in Abb. 8 sämtlich Attribute zu User1 aus der MySQL-Datenbank abgefragt. Aufgrund der Normalisierung der Daten und der damit einhergehenden Aufteilung auf fünf Tabellen, werden für die Abfrage mehrere kosten- und zeitintensive Join-Operatoren benötigt. Durch diese werden die Userdaten verknüpft. Durch die komplexe Abfragesprache SQL bieten relationale Datenbanken vielfältige Möglichkeiten bezüglich der Datenabfrage.

Wegen des geringen Datenvolumens der beiden Datenbanken sind in Einzelabfragen keine Unterschiede messbar. Die lediglich 15 Datensätze umfassen zudem nur wenige Attribute, sodass sich keine Performanceunterschiede feststellen lassen. Auch die relationale Daten-

bank kommt mit diesem geringen Datenvolumen problemlos klar. Aus diesem Grund wurden die Abfragen für Testzwecke innerhalb einer Schleife mehrfach wiederholt.Abb. 12zeigt diese Vorgehensweise anhand der Redis-Datenbankabfrage. In diesem wird die Abfrage 100.000fach durchgeführt und das Ergebnis jeweils ausgegeben.

```
for (int i=1; i<2;i++) {

Map<String, String> value = jedis.hgetAll("user5");
System.out.println(value);

}
```

Abb. 12: Wiederholung der Abfrage

Um die vermuteten Performanceunterschiede zwischen der relationalen Datenbank und der Key-Value-Datenbank festzustellen, wurden die Wiederholungszahlen der Abfragedurchläufe variiert und dabei die Durchlaufzeit der beiden Implementierungen gemessen und auf der Konsole ausgegeben. Für diese Testzwecke wurde auf die Ausgabe der Datensätze zunächst verzichtet.

Abb. 13: Messung der Durchlaufzeiten

Oben stehendes Diagramm in Abb. 13zeigt, dass die Durchlaufzeiten der Redis- und der MySQL-Datenbank mit wachsender Anzahl der Durchläufe der Abfragen ansteigt. Dabei wurde berücksichtigt, dass nach jeder Abfrage der Cache gelöscht wird. Weiterhin wurde durch das mehrmalige Ausführen der Abfragen ein Mittelwert der ermittelten Zeiten gebildet, um eventuelle Schwankungen auszugleichen. Es wird deutlich, dass die relationale Daten-

bank bei wenigen Durchläufen noch mit der Redis-Datenbank mithalten kann, mit steigender Durchlaufanzahl die Schere jedoch immer weiter auseinander geht.

Die auf Handhabung großer Datenmengen optimierte Key-Value-Datenbank kann somit mit wachsender Durchlaufzahl ihre Vorteile ausspielen. Grund dafür sind unter anderem die weniger komplexen Abfragen. Unter Berücksichtigung des Projektumfangs und der verwendeten Datenmenge, sind diese Messwerte allerdings mit Vorsicht zu genießen. Sie könnten in einer größer angelegten Testreihe nochmals verifiziert werden.

Davon abgesehen weist auch die Redis-Datenbank einige Nachteile gegenüber der relationalen Datenbank auf. Bei der Abfrage von Datensätzen kann in Redis nicht ohne weiteres nach bestimmten Attributen oder Values suchen. Die Datenbank ist auf die Suche nach einem Key optimiert. Um einen Hashtypen nach einem Wert zu durchsuchen, müsste dafür manuell ein Index angelegt werden. Der Index stellt einen Zugangspfad von den gesuchten Values zum dazugehörigen Key dar.[39] Die relationale Datenbank bietet hingegen die Möglichkeit nach beliebigen Werten zu suchen. Dies wird unter anderem durch die komplexe Abfragesprache SQL ermöglicht. Sie bietet die Möglichkeit nach bestimmten Values zu suchen und auf diesen zusätzlich mathematische Funktionen auszuführen.

Des Weiteren wurden in den Tests bei der einfachen Ausgabe der Datensätze Auffälligkeiten deutlich. Die Methode HGetAll(Key) für die Redis-Datenbank führt zu einer ungeordneten Ausgabe der einzelnen Attribute. Weder eine alphabetische Reihenfolge noch die Reihenfolge entsprechend der Eingabe in die Datenbank sind in der Ausgabe zu erkennen.

Ein genereller Unterschied zwischen den beiden Modellen liegt im jeweiligen Schema. Da die Redis-Datenbank als Vertreter der Key-Value-Stores schemafrei ist, lassen sich für einzelne User problemlos weitere Attribute ergänzen. Die MySQL-Datenbank als Vertreter der relationalen Datenbanken ist dahingegen schemagebunden. Die Datensätze werden in durch die Tabellen vordefinierte Strukturen eingefügt. Das Hinzufügen weiterer Attribute zu einzelnen Usern ist ohne Anpassung der Tabellen nicht möglich. Des Weiteren sind bei Key-Value-Datenbanken unstrukturierte Daten möglich, während relationale Datenbanken vorgegebenen Datentypen unterliegen.

[39] Beispiel zur Anlage eines Index: http://stackoverflow.com/questions/11470468/how-to-search-in-redis-for-hash-keys

Zusammenfassend konnten durch den Vergleich folgende Hauptunterschiede zwischen NoSQL-Datenbanken und relationalen Datenbanken festgestellt werden:

	NoSQL (Redis)	Relational (MySQL)
Aufbau	Einfacher Hashwert	Normalisierte Tabellen
Abfragekomplexität (API)	Niedrig	Hoch
Durchlaufzeit	Vorteile bei vielen Anfragen	Probleme bei steigender Anzahl der Anfragen
Schema	Schemafrei	Schemagebunden

Tabelle 11: Vergleich NoSQL vs. Relational

Weitere Eigenschaften von NoSQL-Datenbanken konnten in diesem Vergleich aufgrund des geringen Umfangs nicht getestet werden. Hierzu zählt beispielsweise das Verhalten bei der horizontalen Skalierung der Daten über mehrere Knoten.

Das abschließende nächste Kapitel nimmt eine Zusammenfassung dieser Arbeit vor und liefert einen Ausblick für kommende Entwicklungen in diesem Bereich.

5 Zusammenfassung und Ausblick

Dieses Kapitel reflektiert das Vorgehen dieser Arbeit und deren zentrale Ergebnisse in Form des Kriterienkataloges und des prototypischen Vergleichs. Zudem werden Anregungen für kommende Projekte in diesem Themenbereich sowie ein Ausblick zum Thema NoSQL gegeben.

Zu Beginn dieser Arbeit wurde anhand einer Quellensuche und Internetrecherche die Einarbeitung in das Thema NoSQL-Datenbanken und speziell die Key-Value-Stores vorgenommen. Bereits nach kurzer Zeit wurde deutlich, dass aufgrund der Aktualität der NoSQL-Bewegung wenig Literatur zu diesem Thema verfügbar ist. Aus diesem Grund wurden verstärkt Internetquellen, speziell die Homepages der diversen Anbieter von Key-Value-Datenbanken, genutzt. Auf Basis dieser Recherche wurde eine geschichtliche Einordnung von NoSQL-Datenbanken vorgenommen sowie eine genauere Definition des Begriffs NoSQL und eine Kategorisierung der verschiedenen Arten durchgeführt.

Für den Kriterienkatalog wurden zunächst grundlegende Begriffe zum Thema Key-Value-Stores erläutert, die zum besseren Verständnis des Kriterienkataloges dienen. Hierbei handelte es sich um folgende Begriffe:

- MapReduce
- CAP-Theorem und BASE
- Konsistentes Hashing
- Multiversion Concurrency Control

Anschließend wurde eine Auswahl der zu untersuchenden Systeme getroffen. Diese belief sich auf die sechs Vertreter Redis, BerkeleyDB, Memcached, DynamoDB, Ehcache und Riak. Diese Systeme wurden anhand der Kategorien des Kriterienkataloges systematisch untersucht und deren Einsatzmöglichkeiten dargestellt.

Für den prototypischen Vergleich wurde zunächst ein Benutzerforum als geeignetes Anwendungsszenario ausgewählt. Basierend darauf kristallisierte sichRedis als geeignetes Datenbanksystem aus dem Bereich der Key-Value-Stores heraus. Die relationale Umsetzung erfolgte durch eine MySQL-Datenbank. Grundlegende Unterschiede der beiden Systeme zeigten sich in den Bereichen des Datenbankentwurfs, der Abfragekomplexität, der Durchlaufzeit bei vielen Anfragen sowie der Schemafreiheit bzw. Schemagebundenheit.

Ziel dieser Arbeit war es, grundlegende Unterschiede zwischen relationalen und NoSQL-Datenbanken mit Hilfe des Vergleichs herauszufinden. Dies konnte mit den zur Verfügung stehenden Mitteln und der gegebenen Projektzeit erreicht werden.

Als Fazit zu dem durchgeführten Vergleich ist zu sagen, dass aufgrund der geringen Datenmenge keine umfassenden Erkenntnisse gewonnen werden konnten. Einige grundlegende Unterschiede zwischen relationalen und NoSQL-Datenbanken konnten dennoch aufgezeigt werden. Für die Untersuchung weitergehender Aspekte und die Verifizierung der erzielten Ergebnisse muss in zukünftigen Projekten auf eine größere Datenmenge zurückgegriffen werden. Somit ließen sich aussagekräftigere Ergebnisse hinsichtlich der Durchlaufzeiten sowie möglicherweise das Verhalten beim Einsatz mehrerer Knoten sowie parallelen Zugriffen testen. Dies würde auch zum eingangs beschriebenen Einsatzgebiet von NoSQL-Datenbanken im Bereich von BigData passen, wo relationale Systeme an ihre Grenzen stoßen.

Da sich die Datenmenge wie bereits in Kapitel 2.2 erwähnt alle zwei Jahre verdoppelt, ist mit einem zunehmenden Wachstum des Interesses am Thema NoSQL zu rechnen. Die aufgezeigten Stärken, aber auch Schwächen, die in Kapitel 4.2 anhand von Redis gezeigt wurden,

lassen vermuten, dass der Einsatz von NoSQL-Datenbanken ein wichtiger Punkt in der Zukunft sein wird. Aufgrund der existierenden Schwächen ist nicht davon auszugehen, dass die relationalen Datenbanken abgelöst werden, in bestimmten Anwendungsfällen jedoch der bevorzugte Einsatz von NoSQL-Datenbanken sinnvoll sein wird. Der gezielte Einsatz dieser Systeme kann einen erheblichen Mehrwert in Form von Zeit- und Kosteneinsparungen durch sich ergebende Möglichkeiten wie die horizontale Skalierung bieten.

Quellenverzeichnisse

Literaturverzeichnis

Edlich, S. u.a. (2010):	NoSQL: Einstieg in die Welt nichtrelationaler Web 2.0 Datenbanken, (Hrsg.: Edlich, S., Friedland, A., Hampe, J., Brauer, B.),München: Carl Hanser Verlag
Redmond, E., Wilson, J. (2012)	Sieben Wochen, sieben Datenbanken – Moderne Datenbanken und die NoSQL-Bewegung, Köln: O'Reilly Verlag
Sadalage, P., Fowler, M. (2013)	NoSQL Distilled – A Brief Guide to the Emerging World of Polyglot Persistence, New Jersey: Addison-Wesley

Verzeichnis der Internet- und Intranet-Quellen

FH Köln (2013):	Key/Value-Datenbanksysteme, wikis.gm.fh-koeln.de/wiki_db/Datenbanken/KeyValueSysteme, Abruf: 17.01.2014
Niemann, C. (2011):	Big Data: Herausforderung für Datenbanken, http://www.zdnet.de/41558518/big-data-herausforderung-fuer-datenbanken/, Abruf: 23.12.2013
NoSQL-Database (o.J.):	List of NoSQL Databases, http://www.nosql-database.org, Abruf: 23.12.2013
Pientka, F. (2011):	Datenbanken: NoSQL im BigData-Land, http://www.it-daily.net/it-strategie/enterprise-it/5250-datenbanken-nosql-im-bigdata-land, Abruf: 23:12.2013
Schnelle, J. (2010):	NoSQL- Jenseits der relationalen Datenbanken, http://www.pro-linux.de/artikel/2/1455/nosql-jenseits-der-relationalen-datenbanken.html, Abruf: 23.12.2013
Smith, S. (2012)	NoSQL for ERP, http://smist08.wordpress.com/2012/01/28/nosql-for-erp/, Abruf: 17.01.2014
Solid IT (2014 a):	DB-Engines Ranking von Key-Value-Stores, http://db-engines.com/de/ranking/key-value+store, Abruf: 08.01.2014

Solid IT (2014 b): Berechnungsmethode der Wertungen im DB-Engines Ranking, http://db-engines.com/de/ranking_definition, Abruf: 08.01.2014

Solid IT (2014 c): DB-Engines Ranking-Trend der Key-Value Stores Popularität, http://db-engines.com/de/ranking_trend/key-value+store, Abruf: 08.01.2014

Strozzi, C. (2010): NoSQL – A Relational Database Management System, http://www.strozzi.it/cgi-bin/CSA/tw7/I/en_US/NoSQL/Home%20Page, Abruf: 17.01.2014

Walker-Morgan, D. (2010): NoSQL im Überblick, http://www.heise.de/open/artikel/NoSQL-im-Ueberblick-1012483.html, Abruf: 23.12.2013

SonstigeLiteratur

Brewer, E. (2000): Towards Robust Distributed Systems, PODC 19.07.2000

Gilbert, S., Lynch, N. (2002): Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services

Karger, D. u.a. (1997): Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web, (Hrsg.: Karger, D., Lehman, E., Leighton, T., Levine, M., Lewin, D.,Panigrahy, R.)

Duale Hochschule
Baden-Württemberg
Stuttgart

NoSQL-Datenbanksysteme/-Dienste aus der Cloud

Schriftliche Ausarbeitung
im Rahmen der Lehrveranstaltung „Projekt des 5. Semesters“
Kompetenzzentrum Open Source (KOS)

Vorgelegt von

Marcel Dittkowski
Timm Walz
Tening Njie
Christian Heich

am 31.01.2014

Fakultät Wirtschaft
Studiengang Wirtschaftsinformatik
WWI2011V

Hinweis

Bei vorliegender Ausarbeitung handelt es sich um eine wissenschaftliche Arbeit weshalb, aus Gründen der besseren Lesbarkeit, auf eine geschlechtsspezifische Differenzierung verzichtet wurde. Im Sinne der Gleichbehandlung gelten die verwendeten Begriffe für beide Geschlechter.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AMI	**A**mazon **M**achine **I**mages
AWS	**A**mazon **W**eb **S**ervices
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
CSV	**C**omma-**s**eparated **v**alues
DBMS	**D**aten**b**ank**m**anagement**s**ystem
DHBW	**D**uale **H**ochschule **B**aden-**W**ürttemberg
EC2	**E**lastic **C**loud Computing
EMR	**E**lastic **M**ap **R**eduction
IaaS	**I**nfrastructure **a**s **a** **S**ervice
IP	**I**nternet **P**rotocol
JSON	**J**ava**S**cript **O**bject **N**otation
MVCC	**M**ulti**v**ersion **C**oncurrency **C**ontrol
NIST	**N**ational **I**nstitute of **S**tandardisation and **T**echnology
NoSQL	**N**o **O**nly **SQL**
PaaS	**P**latform **a**s **a** **S**ervice
RDBMS	**R**elationales **D**atenbank-**M**anagement-**S**ystem
SaaS	**S**oftware **a**s **a** **S**ervice

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Wirft man derzeit einen Blick in renommierte IT-Fachzeitschriften, stößt man immer wieder auf den Begriff „NoSQL“ in Verbindung mit Datenbanken. Die sogenannten NoSQL-Datenbanksysteme erleben momentan einen regelrechten Hype und sind in aller Munde. Dies liegt sicherlich an der Tatsache, dass sich der Datenbankbereich schon seit längerer Zeit beruhigt hat und relationale Datenbanksysteme seither als gesetzt galten. Genau diese Vorherrschaft der relationalen Datenbanksysteme wird nun in der Literatur infrage gestellt. Besonders hinsichtlich der Verwaltung und Auswertung von großen Datenbeständen wird den NoSQL-Datenbanksystemen ein großer Vorteil gegenüber relationaler Datenbanksysteme eingeräumt. Diese Tatsache macht diese Art der Datenbanksysteme für viele Unternehmen interessant. Aufgrund ihrer hohen horizontalen Skalierbarkeit, eigenen sich NoSQL-Datenbanksysteme laut ihrer Hersteller besonders für den Einsatz in der Cloud.

Im Verlauf der vorliegenden Forschungsarbeit werden NoSQL-Datenbanksysteme näher betrachtet. Hierzu wird zuerst auf die wichtigsten Konzepte von NoSQL-Datenbanksysteme eingegangen, um die Funktionsweise zu erläutern. Nachfolgend wird der Begriff der NoSQL-Datenbanksysteme mit dem Begriff des Cloud-Computings in einen Kontext gebracht. Anschließend werden konkrete Beispiele für NoSQL-Datenbanksysteme aus der Cloud untersucht. Hierbei wird auf die relevanten Punkte für die Beschaffung und Anwendung solcher Systeme in einem Firmenumfeld eingegangen. Diese Forschungsarbeit nimmt sich zum Ziel, einen Überblick über die Möglichkeiten von NoSQL-Datenbanksysteme aus der Cloud zu schaffen.

2 NoSQL

In diesem Kapitel werden die theoretischen Grundlagen der NoSQL-Datenbanksysteme erläutert und ihre Arbeitsweise vorgestellt.

2.1 Kategorisierung von NoSQL-Datenbanksystemen

NoSQL steht für „*Not only SQL*“ und bezeichnet Datenbanksysteme, die nicht den klassischen relationalen Ansatz verfolgen. Auf der Internetseite „www.nosql-database.org“ befindet sich eine Auflistung aller verfügbaren NoSQL-Datenbanken - momentan (09.12.2013) sind es 150 verschiedene. Um den Überblick zu bewahren erscheint eine Kategorisierung wie sie S. Endlich, A. Friedland, J. Hampe und B. Brauer in ihrem Buch „NoSQL – Einstieg in die Welt nichtrelationaler Web 2.0 Datenbanken“ treffen, sehr sinnvoll. Sie unterteilen die Datenbanken in NoSQL-Kernsysteme und nachgelagerte NoSQL-Systeme.[1]

NoSQL-Kernsysteme:[2]

- Spaltenorientierte Datenbanken
- Dokumentenorientierte Datenbanken
- Key-Value Datenbanken
- Graphenorientierte Datenbanken

Nachgelagerte NoSQL-Systeme:[3]

- Objektdatenbanken
- XML-Datenbanken
- Grid-Datenbanken
- weitere nichtrelationale Systeme

Eine allgemeingültige Abgrenzung von relationalen Datenbanken (SQL) zu NoSQL-Datenbanken ist nicht möglich, wie die nachfolgende Abbildung zeigt. Der Übergang ist fließend.[4]

---

[1] Vgl. Edlich, S./u. a. (2010), S. 6 f.; o. V. (2014a)
[2] Vgl. Edlich, S./u. a. (2010), S. 6 f.
[3] Vgl. Edlich, S./u. a. (2010), S. 6 f.

Abb. 1: Abgrenzung relationaler Datenbanken zu NoSQL-Datenbanken[5]

Zu den ersten echten NoSQL-Systemen gehören HBase und Cassandra (spaltenorientierte Datenbanken), MongoDB (das im späteren Verlauf dieser Arbeit genauer betrachtet wird), CouchDB und Riak (dokumentenorientierte Datenbanken), DynamoDB und Voldemort (Key-Value-Datenbanken).[6]

Aufgrund der zeitlichen Beschränkung bezieht sich diese Arbeit ausschließlich auf die NoSQL-Kernsysteme, die nachfolgend genauer betrachtet werden.

2.1.1 Spaltenorientierte Datenbanken

Spaltenorientierte Datenbanken (Wide Column Stores) speichern Daten mehrerer Einträge in Spalten, ähnlich wie Excel-Tabellen. Dabei besteht jeder einzelne Eintrag aus dem Namen der Spalte, einem Zeitstempel (Timestamp) und den Daten.[7]

---

[4] Vgl. Edlich, S./u. a. (2010), S. 6 f.

[5] Enthalten in: Edlich, S./u. a. (2010), S. 6

[6] Vgl. Edlich, S./u. a. (2010), S. 6

[7] Vgl. Edlich, S./u. a. (2010), S. 7; o. V. (2011a)

Abb. 2: Struktur einer Spalte (spaltenorientierte Datenbank)[8]

Beinhalten Spalten ähnliche Inhalte werden diese in einer sog. „Column Family“ zusammengefasst, wie in Abbildung drei dargestellt wird. Diese haben keine logische Struktur und können aus Tausenden oder sogar Millionen von Spalten bestehen, weshalb sie auch Wide Columns genannt werden.[9]

Abb. 3: Column Family (spaltenorientierte Datenbank)[10]

Ein Vorteil von Wide Columns ist, dass bei dem Leseprozess von Daten keine unnötigen Informationen gelesen und verarbeitet werden müssen, sondern nur diejenigen Daten, die ausgesucht wurden um den Lesezugriff zu beschleunigen. Der Schreibprozess einer einzelnen Spalte profitiert ebenso von diesem Geschwindigkeitsvorteil. Wenn allerdings eine Vielzahl von Daten aus mehreren Spalten geschrieben werden soll, wird der Schreibvorgang verlangsamt, da auf alle relevanten Spalten zugegriffen werden muss.[11]

[8] Enthalten in: o. V. (2011a)
[9] Vgl. o. V. (2011a)
[10] Enthalten in: o. V. (2011a)
[11] Vgl. o. V. (2011a)

Aufgrund der direkten Verarbeitung von Informationen eignen sich spaltenorientierte Datenbanken für analytische Informationssysteme, Data-Mining Systeme, Data Warehouses, Business Reporting und Business Process Management-Systeme.[12]

2.1.2 Dokumentenorientierte Datenbanken

Dokumentenorientierte Datenbanken speichern Daten nicht wie relationale Datenbanken in Tabellen sondern in Dokumenten, wobei hierbei nicht Textdateien gemeint sind, sondern strukturierte Datensammlungen wie z. B. YAML, JSON oder RDF-Dokumente. Dabei werden Felder (Schlüssel) definiert. Jedem Feld wird jeweils ein Wert zugeordnet, der von beliebiger Länge sein kann wie bspw. ein Wort, eine Zahl, ein Text oder eine Datei. Innerhalb eines Dokuments können jederzeit neue Schlüssel mit Werten angelegt werden, da die Dokumente schemalos sind und somit keiner Normalform entsprechen. Aufgrund dieser Schemafreiheit kann jedes einzelne Dokument aus unterschiedlichen Strukturen bestehen. Die Schlüssel müssen innerhalb eines Dokuments einmalig sein, dürfen aber auch in anderen Dokumenten vorkommen.[13]

Abbildung vier zeigt ein Beispiel eines Dokuments im JSON Format.

```
{
"Vorname" : "Max" ,
"Nachname" : "Mustermann" ,
"Telefon-Nr." : "0123456",
"Adresse" : "Musterstraße 34, Musterstadt" ,
"Kinder" :  ["Musterkind1" , "Musterkind2" ] ,
"Alter" :  33
...
}
```

Abb. 4: Dokumentenbeispiel (dokumentenorienterte Datenbank)[14]

[12] Vgl. o. V. (2011a)
[13] Vgl. o. V. (2010); o. V. (2013a); Edlich, S./u. a. (2010), S. 8
[14] Enthalten in: o. V. (2013a)

Aufgrund der Schemafreiheit ergibt sich eine Gestaltungsfreiheit, aus der ein zusätzlicher Aufwand resultiert, da die Struktur der Dokumente selbst definiert und kontrolliert werden muss. Zwischen einzelnen Dokumenten existieren keine Relationen, jedes Dokument ist eine für sich geschlossene Einheit. Die Grundidee von dokumentenorientierten Datenbanken ist die zentrale Speicherung von zusammengehörenden Daten, während im Vergleich dazu relationale Datenbanken die Daten in verschiedenen voneinander getrennten Tabellen abspeichern. Dementsprechend können real existierende Dokumente mit dokumentenorientierte Datenbanken optimal abgebildet werden. Sie eignen sich vor allem für Blogs, Content Management Systeme und Wikis.[15]

2.1.3 Key-Value Datenbanken

Das Schema auf dem Key-Value Datenbanken basieren, besteht aus einem Schlüssel und dem zugehörenden Wert. Der Schlüssel (Key) kann aus einer willkürlichen oder strukturierten Zeichenkette bestehen und in Namensräume oder Datenbanken aufgeteilt werden. Die Werte werden auch Values genannt und können Strings, Sets, Listen oder Hashes enthalten. Mithilfe der nächsten Abbildung werden diese genauer betrachtet.[16]

Abb. 5: Werte Typen (Key-Value Datenbank)[17]

---

[15] Vgl. o. V. (2010); o. V. (2013a)
[16] Vgl. o. V. (2013b)
[17] Enthalten in: o. V. (2013b)

Sets speichern Daten wie Qeues mit der Besonderheit, dass nur von oben auf diese zugegriffen werden kann und dass keine doppelten Werte erlaubt sind. Listen hingegen lassen doppelte Werte zu, ein Zugriff von oben und unten ist möglich wie in der Abbildung zu sehen ist. Bei Hashes wird unter einem Key ein Value und ein Hashwert abgespeichert.[18]

Ein Vorteil dieser Datenbanken ist die Skalierbarkeit sowie das einfache Datenmodell, das eine schnelle und effiziente Datenverwaltung ermöglicht. Die Abfragemächtigkeit ist hingegen oft eingeschränkt, da der Zugriff auf die Daten über dessen Schlüssel erfolgt.[19]

2.1.4 Graphenorientierte Datenbanken

Graphenorientierte Datenbanken sind auf vernetzte Informationen spezialisiert, die in Graph- oder Baumstrukturen organisiert werden und eine möglichst effiziente und einfache Traversierung erlauben. Bei der Traversierung wird meistens ein anderer Knoten gesucht, indem der Graph von einem Startknoten durchlaufen wird. Anwendungsfelder solcher Datenbanken sind klassischerweise Geoinformationssysteme mit denen der kürzeste Weg errechnet werden soll oder „Wer kennt wen"-Beziehungen in sozialen Netzwerken.[20]

Abb. 6: Beispiel eines Graphen (graphenorientierte Datenbank)[21]

[18] Vgl. o. V. (2013b)

[19] Vgl. Edlich, S./u. a. (2010), S. 7; o. V. (2013b)

[20] Vgl. Edlich, S./u. a. (2010), S. 8; o. V. (2013c)

[21] Enthalten in: o. V. (o. J.)

Abbildung sechs zeigt einen Beispielgraphen mit einer „Wer kennt wen“-Beziehung. Dem Beispiel ist zu entnehmen, dass Alice 18 Jahre alt ist und den 22 Jahre alten Bob seit dem 03.10.2001 kennt. Warum hingegen Bob Alice erst seit dem 04.10.2001 kennt ist unklar, lässt aber das Datum des „Freundewerdens“ in einem sozialen Netzwerk vermuten. Des Weiteren zeigt der Knoten ID:3, dass beide in derselben Schachgruppe tätig sind.

2.1.5 Vergleich der Eigenschaften von NoSQL-Kernsystemen

Nachdem die NoSQL-Kernsysteme vorgestellt wurden, werden die Eigenschaften dieser abschließend tabellarisch gegenübergestellt.

Relationale DB	Server	Database	Table	Primary Key			
KeyValue DB	Cluster	Keyspace		Key	Value		
Column Family DB	Cluster	Table/ Keyspace	Column Family	Key	Column Name	Column Value	Super Column optional
Document DB	Cluster	Docspace		Doc Name	Doc Content		
GraphDB	Server	Graphspace	Nodes & Links				

Abb. 7: Gegenüberstellung der NoSQL-Kernsysteme[22]

Neben unterschiedlichen Eigenschaften unterscheiden sich NoSQL-Datenbanken auch danach, ob sie verteilt sind oder nicht. NoSQL-Datenbanken wie MongoDB, Cassandra, HBase, Riak, CouchDB, Lounge, Voldemort und Scalaris sind verteilt wohingegen Redis und SimpleDB von Amazon dies nicht sind. Zudem arbeiten die Datenbanken entweder Disk- oder RAM-basiert. Während CouchDB und Riak Disk-basiert arbeiten sind MongoDB, HBase, Cassandra und Redis individuell konfigurierbar.[23]

[22] Enthalten in: Edlich, S./u. a. (2010), S. 9
[23] Vgl. Edlich, S./u. a. (2010), S. 9

2.2 Wichtige Konzepte

Nachfolgend wird auf wichtige Konzepte der NoSQL-Datenbanksysteme eingegangen, die die Arbeitsweise dieser bestimmen. Dabei wird das Map/Reduce-Framework, das CAP-Theorem, BASE, Consistent Hashing, Multiversion Concurrency Control und Paxos näher betrachtet.

2.2.1 Map/Reduce

Alternative Algorithmen, Datenbankenmanagementsysteme und Frameworks helfen bei der Verarbeitung großer Mengen von Informationen und Daten. In diesem Kapitel wird die grundlegende Idee des Map/Reduce-Frameworks vorgestellt, dass von Google Inc. entwickelt wurde und eine parallele Berechnung von Datenmengen im Bereich von mehreren Tera- und Petabytes erlaubt. Das Map/Reduce-Framework basiert auf der Grundidee von funktionalen Programmiersprachen.[24]

Funktionale Programmiersprachen bieten den Vorteil, dass unerwünschte Effekte wie Verklemmungen (deadlocks) oder kritische Wettläufe (race conditions) nicht entstehen können. Zudem verändern funktionale Operationen die vorhandenen Datenstrukturen nicht, da Kopien der Originaldaten erzeugt und verwendet werden. Jede Operation wird auf einer solchen Kopie durchgeführt, weshalb sich unterschiedliche Operationen auf demselben Datensatz auch nicht gegenseitig beeinflussen. Des Weiteren spielt die Reihenfolge der Ausführung von Operationen keine Rolle und ermöglich damit eine Parallelisierung dieser.[25]

Die Verarbeitung von Daten basiert beim Map/Reduce-Framework auf zwei Phasen (Map und Reduce), wie die folgende Abbildung zeigt.[26]

---

[24] Vgl. Edlich, S./u. a. (2010), S. 12
[25] Vgl. Edlich, S./u. a. (2010), S. 12 f.
[26] Vgl. o. V. (2013d)

Abb. 8: Datenfluss beim Map/Reduce-Framework[27]

Als Erstes werden die Eingabedaten auf verschiedene Map-Prozesse verteilt, die jeweils parallel die vom Nutzer bereitgestellte Map-Funktion berechnen. Anschließend werden die Ergebnisse in verschiedene Zwischenergebnisspeicher abgelegt - in der Abbildung durch pinke Sterne illustriert. Sind alle Zwischenergebnisse berechnet, ist die Map-Phase beendet. Daraufhin startet die Reduce-Phase, in der für jedes Zwischenergebnis die vom Nutzer bereitgestellte Reduce-Funktion parallel ausgeführt wird. Jedes daraus resultierende Ergebnis wird als Ergebnisdatei im Dateisystem gespeichert. Sind alle Ergebnisdateien gespeichert, ist die Reduce-Phase und damit die gesamte Ausführung des Map/Reduce-Frameworks abgeschlossen.[28]

Zu beachten ist dabei, dass der Anwender die Logik seiner Anwendung durch die Erstellung der benötigten Map- und Reduce-Funktion selbst definiert. Die beteiligten Prozesse, die Verteilung der Daten und die Speicherung der Zwischen- und Endergebnisse werden vom Map/Reduce-Framework übernommen. Diese Trennung von Anwendungslogik und technischer Seite erlaubt es dem Anwender sich auf die Lösung seines Problems zu konzentrieren.[29]

Um die Arbeitsweise des Map/Reduce-Frameworks konkret anhand eines praxisbezogenen Beispiels zu verdeutlichen, wird ein Beispiel herangezogen, bei dem es um die Auswertung von Wetterdaten geht. Das Ziel ist es, aus unstrukturierten Wet-

---

[27] Enthalten in: o. V. (2013d)
[28] Vgl. Edlich, S./u. a. (2010), S. 17
[29] Vgl. Edlich, S./u. a. (2010), S. 17

terdaten die jährlichen Temperatur-Maxima in einer Datei auszugeben. Dabei werden zu Beginn die unstrukturierten Wetterdaten eingelesen.[30]

- 0029029070999991901010106004+6433 … 059
  9999V0202701N015919999999N0000001 … 00
  1ADDGF108991999999999999999999
- 0029029070999991901010113004+64333+023450FM-12+000059
  9999V0202901N008219999999N0000001N9-00721+9999910200
  1ADDGF104991999999999999999999

Abb. 9: Map/Reduce Beispiel Schritt 1: Einlesen der unstrukturierten Wetterdaten[31]

Nachdem die Daten eingelesen wurden, werden die Inhalte verschiedenen Positionen zugeordnet und mittels der Map-Funktion transformiert. Hierbei entstehen Key/Value-Paare wie die nächste Abbildung zeigt.[32]

Jahr	Temperatur
1950	0
1950	22
1949	111
1949	78

Abb. 10: Map/Reduce Beispiel Schritt 2: Transformation der Daten mittels der Map-Funktion I[33]

Anschließend werden in der Map-Funktion die Key/Value-Paare gruppiert, sortiert und die Werte jeweils einem Schlüssel zugeordnet. Danach werden die Ergebnisse im Zwischenergebnisspeicher abgelegt und die Reduce-Funktion beginnt.[34]

Jahr	Temperatur
1949	111
	78
1950	0
	22

Abb. 11: Map/Reduce Beispiel Schritt 3: Transformation der Daten mittels der Map-Funktion II[35]

---

30 Vgl. Findling T./König, T. (o. J.), S. 10 ff.
31 Enthalten in: Findling T./König, T. (o. J.), S. 10
32 Vgl. Findling T./König, T. (o. J.), S. 10 ff.
33 Enthalten in: Findling T./König, T. (o. J.), S. 12
34 Vgl. Findling T./König, T. (o. J.), S. 10 ff.

Mit der Reduce-Funktion werden die Werte in einer Ergebnisdatei zusammengefasst, sodass pro Schlüssel nur noch ein Wert existiert – das jeweilige Maximum.[36]

Jahr	Temperatur
1949	111
1950	22

Abb. 12: Map/Reduce Beispiel Schritt 4: Zusammenfassung der Werte mittels der Reduce-Funktion[37]

Weitere Anwendungsbereiche des Map/Reduce-Frameworks sind bspw.[38]

- Verteiltes Suchen (Grep)
- Zählen von Zugriffen auf eine URL
- Wortindex Erstellung
- Sortieren verteilter Daten
- Kategorisierung von Daten zur Nachrichtenaufbereitung
- Auswertung beliebiger Logdateien
- Aufbereitung von Daten für häufige Aufrufe

Im Kontext der NoSQL-Datenbanksysteme spielt das Map/Reduce-Framework eine zentrale Rolle da es, wie schon bereits erwähnt, eine effiziente und parallele Ausführung von großen und verteilten Datenmengen ermöglicht. Dementsprechend wird es von mehreren NoSQL-Datenbanksystemen wie bspw. MongoDB, Riak, CouchDB und HBase verwendet.[39]

2.2.2 Cap-Theorem

Das Cap-Theorem – auch Brewer's Theorem genannt – besagt, dass eine vollständige Vereinbarkeit der drei Eigenschaften *Konsistenz* (Consistancy), *Verfügbarkeit* (Availability) und *Ausfalltoleranz* (Partition Tolerance) nicht gewährleistet werden

[35] Enthalten in: Findling T./König, T. (o. J.), S. 13
[36] Vgl. Findling T./König, T. (o. J.), S. 10 ff.
[37] Enthalten in: Findling T./König, T. (o. J.), S. 14
[38] Vgl. Edlich, S./u. a. (2010), S. 22 f.
[39] Vgl. Edlich, S./u. a. (2010), S. 28 f.

kann. Die Kernaussage des Cap-Theorems ist somit, dass ein verteiltes System maximal zwei dieser drei Eigenschaften gleichzeitig erfüllen kann. Bezogen auf Datenbanken die eine möglichst hohe Verfügbarkeit und Ausfalltoleranz bieten sollen bedeutet dies, dass es notwendig ist die Anforderungen an die Konsistenz zu lockern. Das Theorem ist für das Verständnis von NoSQL-Datenbanksystemen unerlässlich. Deswegen werden mithilfe der nächsten Abbildung die Grundgrößen näher erläutert.[40]

Abb. 13: Cap-Theorem[41]

Konsistenz (Consistancy) bedeutet für verteilte Datenbanken das im Abschluss einer Transaktion die verteilten Daten einen konsistenten Zustand erreichen. Ein verteiltes Datenbanksystem mit mehreren replizierenden Knoten ist dann konsistent, wenn nach einer Transaktion die bspw. einen Eintrag in einer Tabelle vornimmt, alle nachfolgenden Lesezugriffe (egal über welchen Knoten) den aktualisierten Wert zurückliefern. Der geänderte Wert kann also erst dann gelesen werden, wenn alle Knoten aktualisiert sind. Bei einem großen Cluster mit vielen Knoten kann dies einiges an Zeit

[40] Vgl. Edlich, S./u. a. (2010), S. 31 f.
[41] Enthalten in: Brown, C. (2011)

beanspruchen. Unter der Verfügbarkeit (Availability) wird eine akzeptable Reaktionszeit verstanden, die von Anwendung zu Anwendung variieren kann. Gerade für viele E-Commerce-Anwendungen ist die Verfügbarkeit ein kritisches Systemmerkmal, da sie einen direkten Einfluss auf Geschäftsentwicklungen haben. Die Ausfalltoleranz (Partition Tolerance) bedeutet, dass der Ausfall einzelner Knoten bei verteilten Datenbanken nicht zum gesamten Ausfall des Systems führt, sondern das das System weiterarbeitet und weiterhin auf Anfragen von außen reagieren kann.[42]

2.2.3 BASE

Als Gegenpart zum klassischen ACID Modell von relationalen Datenbank-Management-Systemen (RDBMS) versteht sich das Base Modell von NoSQL Datenbanken. BASE steht für *Basically Available*, *Soft State* und *Eventually Consistent* und wird zur Lösung des aus dem CAP-Theorem resultierenden Konflikts herangezogen. Basically Available bedeutet, dass das System grundsätzlich verfügbar ist und das ein Ausfall einzelner Teile toleriert wird. Mit Soft State und Eventually Consistent ist gemeint, dass das System nach einer Transaktion nicht konsistente Daten enthält und der Status der Konsistenz irgendwann erreicht wird. Deswegen können im Laufe einer Transaktion inkonsistente Zustände auftreten, was bei klassischen relationalen Datenbank-Management-Systemen nicht möglich ist. Dies gilt es beim Einsatz von NoSQL Datenbanken zu berücksichtigen.[43]

2.2.4 Consistent Hashing

Consistent Hashing ist eine spezielle Art des Hashing und stellt ein weiteres zentrales Konzept der NoSQL-Datenbanksysteme dar. Genau wie beim Standard-Hashing wird das Consistent Hashing verwendet, um eine große Eingabemenge (Keys) auf eine kleinere Zielmenge (Hashes) abzubilden.[44]

Das wohl einfachste und gleichzeitig bekannteste Beispiel einer Hash-Funktion ist die Modulo-Funktion. Die Modulo-Funktion liefert dabei den Rest bei einer ganzzahligen Division. So ermittelt bspw. die Funktion 7 mod 3 den Rest 1. Die Funktion

[42] Vgl. Edlich, S./u. a. (2010), S. 31 f.
[43] Vgl. Edlich, S./u. a. (2010), S. 33 ff.
[44] Vgl. Edlich, S./u. a. (2010), S. 36

mod 3 bildet eine beliebige Eingabemenge auf insgesamt 3 Hashes ab. Die Anzahl der Hashes entspricht der Anzahl der möglichen Ergebnisse der jeweiligen Hashfunktion. In Abb. 14 ist das Hashen durch die Modulo-Funktion mod 3 abgebildet. Dabei wird die Eingabemenge auf vier Hashes abgebildet.

Abb. 14: Hashfunktion Modulo 3

Hash-Funktionen können vielseitig eingesetzt werden. Anwendungsmöglichkeiten sind beispielsweise die Berechnung von Prüfsummen oder die Herstellung von kryptografischen Schlüssel.[45]

Im Zusammenhang mit Datenbanken werden Hash-Funktionen jedoch in einem anderen Kontext verwendet. Hier werden sie verwendet, um Objekten einen festen Speicherort zuzuweisen. Ein Hashwert entspricht im Normalfall einem Speicherort (z. B. Server). Das Konzept des Hashens soll meist auch sicherstellen, dass Objekte möglichst gleich auf die unterschiedlichen Speicherorte verteilt werden. Dies kann gewährleistet werden, wenn die einzelnen Hashes als Ergebnis die gleiche Häufigkeit besitzen.[46]

An dieser Stelle wird das Consistent Hashing relevant. Es flexibilisiert den konventionellen Ansatz des Hashens, um Hashfunktionen auch im Zusammenhang mit NoSQL-Datenbanksysteme nutzbar zu machen. Der Grund, warum das konventionelle Hashen für die Verwendung in NoSQL-Datenbanksystemen nicht geeignet ist, resultiert aus der Tatsache, dass sich NoSQL-Datenbanken durch ihre hohe Skalier-

[45] Vgl. Edlich, S./u. a. (2010), S. 36
[46] Vgl. Edlich, S./u. a. (2010), S. 37

barkeit auszeichnen. Die zentrale Idee der NoSQL-Datenbanken ist es, dass sich der Speicherplatz auf einzelne Server mit unterschiedlichen Kapazitäten aufteilt. Dabei gewährleistet das Datenbanksystem eine Kompensation von Serverzugängen und Serverabgängen im laufenden Betrieb. Aus diesen Fakten leiten sich zwei Herausforderungen ab, die es mithilfe des Consistent Hashing zu beseitigen gilt.[47]

Als erstes ist anzumerken, dass das konventionelle Hashen einzelne Keys in festgelegte Hashes abbildet. Durch ständige Serverzugänge und Serverabgänge variiert die Anzahl der Hashes jedoch sehr stark bei NoSQL-Datenbanken. Ändert sich die Anzahl der Server, müssten unter der Verwendung des konventionellen Hashens sämtliche Objekte erneut auf die variierte Anzahl der Hashes verteilt werden. Für NoSQL-Datenbanksysteme muss deshalb ein Hash-Verfahren verwendet werden, bei dem bei Serverzugängen und Serverabgängen nur ein kleiner Teil der Objekte neu verteilt werden muss.[48]

Die zweite Problematik, derer sich das Consistent Hashing annimmt, resultiert aus der Unterschiedlichkeit der Server, aus denen der Speicherplatz einer NoSQL-Datenbank besteht. Die Server können sich besonders hinsichtlich ihrer Kapazitäten unterscheiden. Das konventionelle Hashen kann sicherstellen, dass eine Menge von Objekten gleichmäßig auf Speicherorte gleicher Kapazität verteilt wird. Dabei werden die unterschiedlichen Speicherorte gleichermaßen ausgelastet. Unterscheiden sich die Speicherorte eines Systems jedoch hinsichtlich ihrer Kapazität, kann eine Gleichverteilung nicht gewährleistet werden.[49]

Um die genannten Problematiken zu beseitigen, verwendet das Consistent Hashing folgenden Ansatz. Die verschiedenen Server werden gemäß ihres Hash-Werts, für den sie zuständig sind, auf einem Ring angeordnet. Im nächsten Schritt können die Objekte je nach Hash-Wert eingefügt werden. Der Server der für ein Objekt zuständig ist, befindet sich im Uhrzeigersinn nächstgelegen. Das Modell ist in Abb. 15 abgebildet.[50]

---

[47] Vgl. Edlich, S./u. a. (2010), S. 37
[48] Vgl. Edlich, S./u. a. (2010), S. 37
[49] Vgl. Edlich, S./u. a. (2010), S. 38 f.
[50] Vgl. Edlich, S./u. a. (2010), S. 38

Abb. 15: Server und Objekte auf einem Ring[51]

Das Hinzufügen oder Entfernen eines Servers kann durch die Abbildung als Ring auf eine einfache Weise kompensiert werden. Das Consistent Hashing stellt sicher, dass solche Änderungen sich nur auf Server und Objekte auswirken, die sich in unmittelbarer Umgebung der Änderungen befinden. Wird ein zusätzlicher Server zum Ring hinzugefügt, so werden ihm alle Objekte zugeordnet, die sich zwischen seinem eigenen und dem Hash-Wert seines Vorgängers befinden. Das Entfernen eines Servers aus dem System ist ähnlich simpel abgebildet. Ein Server der den Ring verlässt kopiert zuvor sämtliche Objekte, die ihm zugeordnet sind, zum nachfolgenden Server. In Abb. 16 ist das Hinzufügen bzw. das Entfernen von Servern schematisch dargestellt.[52]

Abb. 16: Hinzufügen und Entfernen von Servern[53]

[51] Enthalten in: Edlich, S./u. a. (2010), S. 38
[52] Vgl. Edlich, S./u. a. (2010), S. 38
[53] Enthalten in: Edlich, S./u. a. (2010), S. 39

Die Unterschiedlichkeit von Servern hinsichtlich ihrer Kapazität oder Perfomance wird vom Consistent Hashing ebenfalls berücksichtigt. Dazu verwendet das Consistent Hashing folgenden Ansatz. Für Server, die eine höhere Kapazität oder Perfomance als die anderen Server des Systems besitzen, können beliebig viele virtuelle Server erzeugt werden. Jedem virtuellen Server werden unterschiedliche Hashwerte zugewiesen. Die virtuellen Server können demnach auch einzeln auf dem Ring platziert werden. Physisch werden die einzelnen Objekte jedoch nur auf einem Server gespeichert. In Abb. 17 ist ein Ring abgebildet, der virtuelle Server beinhaltet.[54]

Abb. 17: Virtuelle Server auf dem Ring[55]

2.2.5 Multiversion Concurrency Control

Die zentrale Aufgabe eines Datenbanksystems ist die Sicherstellung der Datenkonsistenz. Besonders bei Datenbanken, die mehreren Anwendern das Manipulieren von Daten gewähren, sind solche Konzepte relevant. Durch eine Vielzahl an Anwendern kommt es beispielsweise zu Situationen, in denen mehrere Anwender zum gleichen Zeitpunkt dasselbe Objekt einer Datenbank manipulieren möchten. Solche Situationen werden als konkurrierende Zugriffe bezeichnet. Sie entstehen, wenn mehrere Anwender zum gleichen Zeitpunkt auf dasselbe Objekt zugreifen. Der Zugriff erfolgt über Operationen (*Lesen, Hinzufügen, Ändern, Lösche*n). Das gleichzeitige Lesen mehrerer Anwender entspricht dabei keinem konkurrierenden Zugriff.[56]

---

[54] Vgl. Edlich, S./u. a. (2010), S. 39
[55] Enthalten in: Edlich, S./u. a. (2010), S. 39
[56] Vgl. Edlich, S./u. a. (2010), S. 40; o. V. (2011b)

Die etablierte Herangehensweise zu Behandlung von konkurrierenden Zugriffen ist derzeit das pessimistische Sperrverfahren. Das Verfahren erlaubt Anwendern das manipulieren von Objekten erst, wenn das jeweilige Objekt zuvor für andere Anwender gesperrt wird. Möchte ein Anwender beispielsweise den Wert eines bestimmten Objekts abändern, so muss er das jeweiligen Objekt zuvor sperren (Lock setzen). Nachdem der Anwender seine Änderung durchgeführt hat, entfernt er die Sperre. Erst ab diesem Zeitpunkt ist das Objekt wieder für andere Anwender lesbar bzw. schreibbar. Das gleichzeitige Lesen kann ohne ein Sperren der Objekte geschehen. Das Konzept ist in Abb. 18 dargestellt.[57]

Abb. 18: Pessimistisches Schreibverfahren[58]

Heutzutage zeigt sich jedoch, dass das pessimistische Schreibverfahren keine optimale Lösung für neue Anwendungsgebiete ist. Die Wartezeiten, die im pessimistischen Schreibverfahren durch das Sperren generiert werden, sind für moderne Systeme ein Faktor, der nicht akzeptiert werden kann. Aus demselben Grund eignet sich das pessimistische Sperrverfahren nicht für NoSQL-Datenbanksysteme.[59]

NoSQL-Datenbanken bestehen meist aus einer Vielzahl an unterschiedlichen Servern und stellen somit ein verteiltes System dar. Das Sperren von Datensätzen würde in diesem Umfeld einen immensen Zeitaufwand generieren. Außerdem ist der Kommunikationsaufwand, der in einem verteilten System notwendig wäre um eine Übereinkunft über das Setzen von Sperren zu treffen, enorm.[60]

---

[57] Vgl. Edlich, S./u. a. (2010), S. 40

[58] Enthalten in: Edlich, S./u. a. (2010), S. 40

[59] Vgl. Edlich, S./u. a. (2010), S. 41

[60] Vgl. o. V. (2011b)

Trotzdem muss die Konsistenz der Daten auch in einer NoSQL-Datenbank sichergestellt werden. Eine Alternative zum pessimistischen Sperrverfahren ist Multiversion Concurrency Control (MVCC). MVCC versucht nicht die Zugriffe auf die unterschiedlichen Objekte über Sperren zu koordinieren, sondern wählt hierfür einen anderen Ansatz. Das Konzept verwendet unterschiedliche Versionen um konkurrierende Zugriffe zu koordinieren. MVCC kann hierbei grob in die drei Aktionen: *Lesen, Schreiben* und *Aufräumen* untergliedert werden. Das Lesen ist unter MVCC völlig von Schreiboperationen losgelöst. Die MVCC stellt zu diesem Zweck zu jedem Zeitpunkt eine aktuelle Version bereit. Ein Schreibzugriff erstellt unter MVCC eine neue Version des jeweiligen Objekts. Eine zentrale Rolle spielt dabei die Versionsnummer. Nach erfolgreichem Schreibzugriff wird überprüft, ob die Versionsnummer der Vorgängerversion die aktuelle Versionsnummer ist. Ist dies der Fall, kann die Version die durch den Schreibzugriff erstellt wurde als aktuelle Version abgespeichert und die Transaktion als abgeschlossen bezeichnet werden. Wird nach erfolgreichem Schreibzugriff festgestellt, dass die Versionsnummer kleiner ist als die aktuelle Versionsnummer, so liegt ein Konflikt vor. In diesem Fall wird der Schreibzugriff auf eine Version angewendet, die zum Transaktionsende nicht mehr aktuell ist. In den meisten Fällen kann das DBMS die Konflikte auflösen, indem mehrere Versionen miteinander vergleicht werden. Wurden die Änderungen an unterschiedlichen Stellen vorgenommen, so können mehrere Versionen simpel zusammengeführt werden. Ein unlösbarer Konflikt liegt vor, wenn in mehreren Versionen Änderungen an mindestens einem gleichen Objekt vorgenommen werden. Bei Schreibzugriffen, die solche unlösbaren Konflikte erzeugen, wird die Transaktion durch das DBMS abgebrochen. Dem jeweiligen Anwender wird eine Fehlermeldung angezeigt. Die dritte Aktion der MVCC ist das Aufräumen. In regelmäßigen Intervallen müssen veraltete Versionen von Objekten gelöscht werden, um den Speicherplatz einer Datenbank nicht unnötig zu beanspruchen.[61]

[61] Vgl. Edlich, S./u. a. (2010), S. 41; o. V. (2011b)

Abb. 19: Handlungsweise Multiversion Concurrency Control[62]

In Abb. 19 ist die Handlungsweise genauer dargestellt. Die beiden Anwender Alice und Bob führen jeweils einen Lesezugriff und einen nachfolgenden Schreibzugriff auf dieselbe Version durch. Beide Anwender erzeugen eine neue Version. Alice beendet die Bearbeitung zuerst. Ihre Version besitzt ab diesem Zeitpunkt die aktuelle Versionsnummer. Bob versucht erst danach seine Version zu speichern. Seine Änderungen basieren jedoch nicht mehr auf der aktuellsten Version, weshalb er seine Version mit der aktuellsten Version zusammenführen muss.

2.2.6 Paxos

In diesem Abschnitt wird der Begriff Paxos definiert und erläutert. Hierbei wird ausschließlich auf die Motivation zur Anwendung von Paxos eingegangen. Eine Betrachtung auf einer detaillierteren Ebene würde den Rahmen dieser Arbeit sprengen.

Unter dem Begriff Paxos versteht man eine Protokoll-Familie die sich mit dem Anwendungsgebiet der Consensus-Probleme befasst. Das Consensus-Problem betrifft dabei die Herausforderung, die Gesamtheit der Systeme in einer verteilten Architektur verlässlich zu machen. In einem verteilten System, wie es beispielsweise NoSQL-Datenbanken sind, ist dieser Fakt nicht zu vernachlässigen, da einzelne Teilsysteme wie beispielsweise Server ausfallen können.[63]

[62] Enthalten in: Edlich, S./u. a. (2010), S. 42
[63] Vgl. Edlich, S./u. a. (2010), S. 47

An dieser Stelle werden die Paxos Protokolle relevant. Diese sind sehr fehlertolerant und somit ein weiteres Konzept zur Sicherung der Datenkonsistenz. Der Leitgedanke ist dabei, dass der Ausfall eines Teilprozesses nicht die Konsistenz der Daten gefährdet. Beispielsweise muss eine Änderung an einem Objekt einer NoSQL-Datenbank von allen Teilsystemen (Server) getragen werden. Der Fall, dass eine Transaktion an Server 1 abgeschlossen wurde und in Server 2 abgebrochen wurde, darf nicht eintreten. Für die Protokolle der Paxos-Familie genügt es, wenn sich eine Mehrheit auf einen Wert einigt. Ein Beispiel für solch einen Wert ist das Beispiel der Status einer Transaktion.[64]

3 Cloud-Computing

Nachdem die theoretischen Grundlagen, die für das Verständnis der NoSQL-Datenbanksysteme notwendig sind, erarbeitet wurden, befasst sich dieses Kapitel mit Cloud-Computing.

3.1 Definition

Unter dem Begriff Cloud-Computing (englisch für „Rechnen in der Wolke“) werden dynamische Ansätze verstanden, informationstechnische Ressourcen über ein Netzwerk zur Verfügung zu stellen. Zu diesen Infrastrukturen zählen Netze, Speichersysteme, Anwendungen und Dienste. Der Zugriff auf diese Ressourcen soll zu jeder Zeit und standortunabhängig möglich sein. Diese abstrahierte IT-Infrastruktur ist für den Nutzer des Dienstes undurchsichtig. Die Verwendung der Ressourcen wird über definierte Schnittstellen und Protokolle ermöglicht. Der Raum, in dem sich die jeweiligen Ressourcen befinden, wird kurzum als „Cloud“ bezeichnet, während beim Gesamtsystem vom „Cloud-Computing“ gesprochen wird. Die Verwendung des Wortes „Wolke“ gilt als Metapher für ein geographisch weit entferntes Objekt, deren Inhalt die ausgelagerten informationstechnischen Ressourcen darstellen.[65]

Eine weitverbreitete Definition für das Cloud-Computing ist die des National Institute of Standards and Technology (NIST). Es handelt sich dabei um eine in den USA ansässige Bundesbehörde, welche sich unter anderem die Standardisierung von IT-

[64] Vgl. Kuhn, F./Boutellier, R. (2012), S.5
[65] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.11f; BSI (2012), S.14

Konzepten zur Aufgabe gemacht hat. Sie wird bei gravierenden Anwendungen jeweils auf den neuesten Stand angepasst, wodurch sie sich als dynamische Definition auszeichnet.[66]

Ein Cloud-Service wird laut der NIST-Definition durch folgende Eigenschaften charakterisiert.[67]

- **On-demand self-service** (Selbstbedienung bei Bedarf): Kunden, die einen Cloud-Service in Anspruch nehmen und weitere Ressourcen benötigen, können diesen bei Bedarf vom Anbieter anfordern. Es ist dabei keinerlei menschliche Interaktion seitens des Anbieters notwendig. Der Kunde kann über seinen Portal-Zugang die gewünschten Ressourcen buchen, welche dann in der Regel innerhalb weniger Minuten automatisch bereitgestellt werden.
- **Broad Network Access** (Breitbandiger Netzzugang): die Services sind über das Netzwerk (in diesem Falle das Internet) verfügbar und Client-unabhängig. Die Services können demnach von unterschiedlichen Endgeräten über einen aktuellen Browser genutzt werden. Zu diesen Endgeräten zählen beispielsweise stationäre Computer, Notebooks, Tablets und Smartphones.
- **Resource Pooling:** die Ressourcen des Cloud-Dienstes befinden sich in einem Pool, welcher von den Abnehmern beansprucht werden kann. Die Kunden sind sich dabei nicht über den Ort, an dem sich dieser Pool befindet, bewusst.
- **Rapid Elasticity** (schnelle Elastizität): aufgrund der Dynamik der Cloud-Dienste können Ressourcen sofort bereitgestellt werden. Für den Kunden ist der Bereitstellungsvorgang nicht transparent – er erfährt also nicht, woher die zur Verfügung gestellten Betriebsmittel stammen.
- **Measured Services** (Messdienste): die Nutzung der verfügbaren Ressourcen wird gemessen und überwacht. Zu diesen Werten zählen unter anderem das verwendete Speichervolumen, die Prozessorauslastung und die verfügbare Bandbreite des Netzwerks. Von einigen Providern werden diese Informationen veröffentlicht. Dies soll das Vertrauen in den Anbieter seitens der Kunden steigern, da der Kunde dadurch Auskunft über die durchgängige Verfügbarkeit seines gemieteten Systems erhält.

[66] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.12 ff.; BSI (2012), S.14
[67] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.12 ff.; BSI (2012), S.14

3.2 Historie

Cloud-Computing gilt als bedeutendstes Konzept seit der Ablösung der Mainframe-Technologie durch das Client-Server-Modell in den 1980er-Jahren. Letzteres Prinzip wird auch im Cloud-Computing an sich beibehalten. Die Gewichtung verschiebt sich jedoch mehr und mehr in Richtung Server, u. a. da komplette Netzwerkinfrastrukturen in die Cloud ausgelagert werden.[68]

3.3 Typisierung

Gemäß der Definitionen des NIST ist der Begriff “Cloud” in die folgenden verschiedene Ansätze zu unterteilen.[69]

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

3.3.1 Private Cloud

Bei einer *Private Cloud* handelt es sich um eine Infrastruktur, welche ausschließlich für einen Abnehmer vorgesehen wird. Diese muss sich nicht zwangsläufig im Netzwerk des Abnehmers befinden, sondern kann ebenso im Netzwerk einer anderen Institution betrieben werden.[70]

3.3.2 Public Cloud

Eine *Public Cloud* stellt hingegen einen Ansatz dar, dessen Infrastruktur für die Allgemeinheit verfügbar sein soll. Die Ressourcen befinden sich bei einer zentralen Institution und werden für alle Abnehmer von dort aus bereitgestellt.[71]

[68] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.1
[69] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.18; BSI (2012), S.16
[70] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.18; BSI (2012), S.16
[71] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.19; BSI (2012), S.16

3.3.3 Community Cloud

Um mehreren Institutionen, die ähnliche Interessengebiete aufweisen, eine gemeinsame Plattform zur Verfügung stellen, werden sogenannte *Community Clouds* betrieben. Deren Infrastruktur kann sowohl bei einem unabhängigen Anbieter betrieben werden oder sich in den Netzwerken eines Community-Mitglieds befinden.[72]

3.3.4 Hybrid Cloud

Eine weitere Variante stellt die *Hybrid Cloud* dar. Bei dieser Ausprägung werden mehrere, unabhängige Infrastrukturen über gemeinsam definierte Schnittstellen gekoppelt, um eine übergreifende Funktion zu ermöglichen.[73]

3.4 Beweggründe für den Einsatz von Cloud-Diensten

Zahlreiche Unternehmen verzichten aus wirtschaftlichen Gründen auf eine interne IT-Abteilung und geben die Verantwortung an einen externen Dienstleister ab. Dieses Vorgehen wird als Outsourcing bezeichnet. Charakteristisch dafür ist, dass Anbieter von IT-Dienstleistungen für jeden Kunden eine gesonderte IT-Infrastruktur aufbauen und dass diese meistens an Verträge mit längeren Laufzeiten gebunden sind. Bei Cloud-Diensten hingegen teilen sich in der Regel mehrere Abnehmer aufgrund der Wirtschaftlichkeit eine gemeinsame IT-Infrastruktur. Durch diese gemeinsame Verwendung muss bei kurzfristigen Umstellungen nicht die komplette Infrastruktur geändert werden. Ressourcen wie Rechenleistung oder Speicherplatz können flexibel bereitgestellt werden, sofern sie beim Anbieter verfügbar sind. Diese Eigenschaft gestaltet den Cloud-Dienst dynamisch und führt zu geringeren Wartezeiten für die Abnehmer. Zudem bleibt dem Abnehmer der Dienstleistungen in der Regel die Option, die in Anspruch genommenen Cloud-Dienste selbst zu administrieren. Dies geschieht meist über eine Web-Oberfläche, wodurch dieser nicht mit komplexen Prozessen konfrontiert wird.[74]

[72] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.19; BSI (2012), S.16
[73] Vgl. Metzger/C. Reitz, T./Villar, J. (2011), S.19f; BSI (2012), S.16
[74] Vgl. BSI (2012), S.18 ff.

3.5 Cloud-Servicemodelle

Cloud-Computing ermöglicht die Bereitstellung und Verwendung verschiedener Servicemodelle als Web-Dienste. Diese unterschiedlichen Services werden im Wesentlichen in die drei Bereiche Hardware, Betriebssystem und Anwendung unterteilt. Die folgende Abbildung stellt die Services in einem Schichtenmodell dar.[75]

Abb. 20: Die Cloud Services im Schichtenmodell[76]

Anhand des Modells ist ersichtlich, dass die Schichten aufeinander aufbauen und daher physisch voneinander abhängig sind, dennoch werden diese als eigenständige Kategorien behandelt und von den Cloud-Service-Providern unabhängig voneinander angeboten. Bezeichnend für die Breite der Pyramide ist die Mächtigkeit der verschiedenen Schichten.[77]

Die Breite der Schichten stellt die Mächtigkeit dar, daher bildet Infrastructure as a Service (IaaS) als die größte Schicht das Fundament der Pyramide.

[75] Vgl. Baun, C./u. a. (2011), S.29
[76] Mit Änderungen entnommen aus: Baun, C./u. a. (2011), S. 30
[77] Vgl. Baun, C./u. a. (2011), S.29

3.5.1 Infrastructure as a Service

In der Infrastructure as a Service (IaaS) Schicht bieten Cloud-Service-Provider den Nutzern komplette IT-Infrastrukturen an. Dabei werden grundlegende Hardwareressourcen wie beispielsweise Rechenleistung, Speicherplatz und/oder Netzwerkkapazitäten zur Verfügung gestellt. Für kosteneffiziente Angebote werden diese von den IaaS Providern oftmals virtuell bereitgestellt, können aber auch physisch vorliegen. Virtualisierungstechniken ermöglichen es den Anbietern die eigenen Rechenkapazitäten besser auszunutzen und gleichzeitig besser auf die individuellen Bedürfnisse der Kunden reagieren zu können. Diese Dienstleistung wird meistens über ein öffentliches Netzwerk (Internet) zur Verfügung gestellt. Da der in Anspruch genommene Dienst nur die Basis darstellt, ist der Kunde für deren Inhalte selbst verantwortlich. Mittels einer Weboberfläche werden die hierfür notwendigen Funktionen zur Verfügung gestellt. Darunter fallen u. a. „das Anlegen bzw. Beseitigen von Betriebssystem-Abbildern, die Skalierung von beanspruchten Kapazitäten oder die Definition von Netzwerktopologien".[78]

Nach einer Studie der Berkeley Universität in den USA lässt sich IaaS an folgenden Eigenschaften charakterisieren:[79]

- Nahezu unbegrenzte Hardwareressourcen, die bei Bedarf jederzeit zur Verfügung stehen
- Beliebige Skalierbarkeit der Leistung, sofern erforderlich
- Nutzungsabhängige Abrechnung

Das Konzept der IaaS Dienstleistung ist nicht neu, es stammt aus der Zeit der Mainframecomputer. Eine zentrale Stelle, an welcher die Rechenleistung und Speicherung erfolgt, war die Vorstufe von IaaS, aber mit einem entscheidenden Unterschied. Während beim Mainframecomputer das Unternehmen selbst für den Betrieb der Hardware zuständig ist, stellt bei IaaS hingegen der Provider die Instandhaltung sicher.[80]

Insbesondere für kleine und mittelständische Unternehmen ist dieses Geschäftsmodell als kostengünstige Alternative interessant. Der Erwerb, Betrieb und Instandhal-

---

[78] Vgl. Terplan, K./Voigt, C. (2011), S. 145; Baun, C./u. a. (2011), S. 32
[79] Vgl. Terplan, K./Voigt, C. (2011), S. 144 f.
[80] Vgl. Terplan, K./Voigt, C. (2011), S. 145

tung eigener Hardware führt zu hohen Betriebskosten, da für den Eigenbetrieb einer Serverfarm eine konstante Stromversorgung, ein Kühlsystem und Fachpersonal für die Wartung notwendig ist. Mit dem Einsatz von IaaS fallen diese Kostenträger weg. Einer der bekanntesten Dienstleister im IaaS Bereich ist das US-amerikanische Unternehmen Amazon mit ihrem Cloud-Computing Geschäftsbereich Amazon Web Services.[81]

3.5.2 Platform as a Service

In Platform as a Service (PaaS) liefern die Provider ihren Endkunden neben der grundlegenden Infrastruktur weitergehende Services wie eine Laufzeitumgebung. Obwohl PaaS-Dienste auf IaaS-Angebote aufbauen, haben die User lediglich Zugriff auf die Inhalte des PaaS-Services. Daher ist eine Abgrenzung der beiden Geschäftsmodelle schwierig (s. Kapitel 4.3, Abbildung 22). Eine PaaS Umgebung stellt den Nutzern eine Laufzeit- bzw. Entwicklungsumgebung in Form eines Frameworks zur Verfügung. Eine solche Umgebung beinhaltet in der Regel Middleware, Datenbanken und diverse Entwicklungs-Tools. PaaS Services ermöglichen den Usern eigene Anwendungen zu entwickeln, zu testen und zu nutzen. Aufgrund des Bestimmungszwecks der PaaS Dienste gelten vor allem Softwareentwickler und Systemarchitekten als Zielgruppe. Die bekanntesten Anbieter von PaaS Diensten sind zum einen Google mit dem PaaS Dienst „*App Engine*“ und Microsoft mit der „*Windows Azure Platform*“. [82]

Allerdings verwenden die unterschiedlichen PaaS Provider verschiedene Programmiersprachen und Frameworks, sodass eine Portabilität bei Wechselabsichten nicht gegeben ist. Der Nutzer ist somit Providerabhängig. Um eine Abhängigkeit zu vermeiden, ist die Verwendung von offenen Standards durch Open-Source Produkte oder der Einsatz von Frameworks, welche mehrere Provider anbieten, notwendig.[83] Damit hat der Nutzer mehr Freiheiten in der Wahl seiner Cloud-Anbieter. Bisher konnte sich PaaS nicht als Alternative zur herkömmlichen Softwareentwicklung auf

[81] Vgl. Terplan, K./Voigt, C. (2011), S. 145
[82] Vgl. Terplan, K./Voigt, C. (2011), S. 26
[83] Vgl. Terplan, K./Voigt, C. (2011), S. 58

dem Markt etablieren, mit zunehmenden Open Source Lösungen kann die Akzeptanz unter den Softwareentwicklern steigen.[84]

3.5.3 Software as a Service

Software as a Service (SaaS) ist ein Cloud-Computing Modell, bei dem alle vorherigen Schichten zum Tragen kommen. SaaS beschreibt die Nutzung von Applikationen aus der Cloud heraus. Der Anwender kann mittels eines herkömmlichen Webbrowsers mit der Anwendung interagieren. Da für nahezu alle Betriebssysteme ein Webbrowser verfügbar ist, hat ein Webinterface den Vorteil der Plattformunabhängigkeit. Somit ist eine lokale Installation der Applikation auf dem Endgerät des Benutzers nicht mehr notwendig. Durch die Interaktion mit der Anwendung über einen Webbrowser ist die Zugriffsmöglichkeit, Flexibilität und Mobilität für die Endanwender erhöht. Analog zu IaaS spart sich ein Unternehmen die Kosten einer IT-Infrastruktur und bietet sich daher als eine kostengünstige Alternative an.[85]

3.6 Clouds in Verbindung mit Datenbanken

Mittlerweile befinden sich zahlreiche Anbieter auf dem Markt für NoSQL-Lösungen, weshalb ein breit gefächertes Angebot vorzufinden ist. Diese Dienstleister bieten den Kunden, welche Privatpersonen als auch Unternehmen sein können, eine vorgefertigte NoSQL-Datenbankumgebung an. Vorteilhaft an dieser Variante ist, dass der Kunde sich hierbei nicht um die Verfügbarkeit oder die Funktion auf Betriebssystem- und Anwendungsschicht kümmern muss. Die Anwendung ist in der Infrastruktur des Dienstleisters (u. a. auf dessen Servern) implementiert und wird vom Kunden über das Internet abgerufen. Es handelt sich bei diesen Produkten in der Regel um Lösungen, deren durchgängige Verfügbarkeit vom Provider gewährleistet wird. Das System fungiert transparent gegenüber dem Kunden. Somit sind die niedrigen Schichten der Architektur für ihn nicht einsehbar. Für ihn ist lediglich die Anwendung an sich zugänglich, welche er beansprucht. Dabei bleibt ihm jedoch ein gewisser Spielraum hinsichtlich der Konfiguration seiner „gebuchten" Anwendung. Dadurch muss die Privatperson oder der Mitarbeiter/die Mitarbeiterin nur Kenntnisse in der

[84] Vgl. Terplan, K./Voigt, C. (2011), S. 155
[85] Vgl. Metzger, C./Reitz, T./Villar, J. (2011), S. 21 f.

Bedienung der jeweiligen Anwendung besitzen und kein tiefer gehendes, technisches Know-How.[86]

Für die eben beschriebene Serviceform gibt es wie die folgende Tabelle zeigt, verschiedene Anbieter. Letztere bieten oft unterschiedliche Datenbanksysteme auf ihren Servern an.

Provider	Verwendetes Datenbanksystem
Amazon WebServices	DynamoDB
Microsoft Windows Azure	MongoDB
MongoHQ	MongoDB
ObjectRocket	MongoDB
DataStax	Cassandra
Cloudant	CouchDB

Tabelle 1: Provider für NoSQL-Dienste mit den verwendeten Datenbanksystemen

3.7 Datensicherheit

Das Thema Datensicherheit ist im Zusammenhang mit Cloud-Computing für Unternehmen von großer Bedeutung. Denn alle Daten, die Unternehmen seit ihrer Gründung angesammelt haben, dienen einem bestimmten Verwendungszweck und sind damit fester Bestandteil von Geschäftsprozessen. Letztendlich tragen diese Daten zur Wertschöpfung eines Unternehmens bei. Um wettbewerbsfähig zu bleiben ist es somit wichtig, diese vor der Konkurrenz zu schützen. Aus diesem Grund sorgt der Gedanke, seine Daten physisch auf der Hardware von Cloud-Providern zu lagern, generell für Unsicherheit. Datensicherheit ist daher einer der Schlüsselfaktoren für eine zuverlässige Nutzung von Cloud-Computing.[87]

[86] Vgl. BSI (2012), S.17 ff.
[87] Vgl. BSI (2012), S. 8

Zunächst wird der Begriff Datensicherheit erläutert, welcher sich in zwei Teilbereiche untergliedern lässt:[88]

- Datenschutz
- Informationssicherheit

Gemäß dem Bundesdatenschutzgesetz wird unter *Datenschutz* der Schutz von personenbezogenen Daten vor Missbrauch während der Erhebung, Verarbeitung und Nutzung durch ein computergestütztes System verstanden. Personenbezogene Daten sind Angaben über persönliche oder sachliche Gegebenheiten mit deren Hilfe eine Person aus einer Vielzahl von anonymen Personen identifiziert werden kann.[89]

Aufgabe der *Informationssicherheit* ist es, die Funktionsfähigkeit von Datenverarbeitungssystemen unter Beachtung von Schutzzielen sicherzustellen. Die Schutzziele sind unter anderem die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Daten. Respektive handelt es sich bei Informationssicherheit um Maßnahmen zum Schutz der Daten vor Verlust und Verfälschung. Jedes dieser Schutzziele wird in der Regel durch eine Schutzmaßnahme umgesetzt. Die Umsetzung von Sicherheitskonzepten gehört zu den klassischen Aufgaben der IT-Sicherheit.[90]

Schutzziele

Die Datenhaltung durch eine Cloud in einem öffentlichen Netzwerk ist zahlreichen Gefahren ausgesetzt. Da auch unternehmensbezogene Daten in der Cloud zugänglich gemacht und verarbeitet werden, sind die Sicherheitsaspekte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu beachten. Für eine zuverlässige Nutzung von Daten im Zusammenhang mit Cloud-Computing sind diese jedoch nicht ausreichend, sodass zusätzlich die Schutzziele Transparenz und Zugriffssteuerung zu berücksichtigen sind. Diese werden im Folgenden erläutert.[91]

Vertraulichkeit:

[88] Vgl. Metzger, C./Reitz, T./Villar, J. (2011), S.47; BDSG (2010), S. 5
[89] Vgl. Metzger, C./Reitz, T./Villar, J. (2011), S.47; BDSG (2010), S. 5
[90] Vgl. Metzger, C./Reitz, T./Villar, J. (2011), S.47; Bothe, S. (2012) S. 37 f.
[91] Vgl. Terplan, K./Voigt, C. (2011), S. 78 ff.; BSI (2012) S.29

Das Ziel der Vertraulichkeit dient dem Schutz der Daten vor Einsichtnahme durch unberechtigte Personen. Zur Gewährleistung der Informationsvertraulichkeit sind Kontrollen für den Zugriff auf die Daten notwendig.[92]

Integrität:

Integrität beschreibt den Schutz der Daten durch Manipulation von unautorisierten Personen oder durch Fehler in der Software. Die Datenintegrität ist im Zusammenhang mit Cloud-Computing nur sichergestellt, wenn der Dienst selber und alle beteiligten Komponenten dieses Ziel erfüllen. [93]

Verfügbarkeit:

Der Begriff Verfügbarkeit steht im Zusammenhang mit Cloud-Computing für eine zuverlässige Funktionsfähigkeit und Erreichbarkeit des Services. Der Endanwender soll die Möglichkeit besitzen jederzeit und von überall aus den Dienst nutzen zu können. Analog zur Integrität ist dieses Ziel erst dann erfüllt, wenn der Nutzer als auch der Cloud-Provider eine hohe Verfügbarkeit aufweisen können.[94]

Authentizität:

Authentizität ist die Gewährleistung eines verlässlicher Transaktionen und Informationsaustausches zwischen dem Sender und Empfänger. Die Erfüllung dieses Ziels ist durch eine Authentifizierung mittels digitalen Zertifikaten oder Passwörtern aller beteiligten Komponenten realisierbar.[95]

Transparenz:

Transparenz im Sinne der Datensicherheit bedeutet, dass der Endanwender jederzeit die Art und Weise der Speicherung der Daten nachverfolgen kann.[96]

---

[92] Vgl. Terplan S. 78 ff.
[93] Vgl. Terplan S. 78 ff.
[94] Vgl. Terplan S. 78 ff.
[95] Vgl. Bothe, S. 41 f.
[96] Vgl. Bothe, S. 41 f.

Zugriffssteuerung:

Die Zugriffskontrolle ist eine Ergänzung zu dem Ziel der Vertraulichkeit. Unter Zugriffkontrolle wird eine Verwaltung der Benutzer mit unterschiedlichen Rechten verstanden, um unbefugte Zugriffe in bestimmte Bereiche der Anwendung zu steuern (Schutzfunktion). Hierfür sind diverse Berechtigungsstufen hinsichtlich der Interaktion mit dem Dienst erforderlich, wie beispielsweise Lese-, Schreib- und Löschoperationen.[97]

4 Auswahl und Beschreibung von NoSQL Cloud-Diensten

Wie bereits beschrieben existieren auf dem Markt für NoSQL-Datenbanksysteme aus der Cloud zahlreiche Anbieter, die meist auf unterschiedliche Datenbank-Engines zurückgreifen.

Aufgrund des begrenzten Umfangs dieser Ausarbeitung und der Übersichtlichkeit handelt diese Ausarbeitung von ausgewählten Providern und Datenbank-Engines. Es sollen die Grundprinzipien von NoSQL-Datenbanken dargelegt werden. Diese werden anhand eines ausgewählten Beispielsystems erläutert.

Um die marktführenden Systeme herauszufinden, wurde die Plattform „DB-Engines“ zurate gezogen. Diese Einrichtung wird von „Solid IT“ betrieben. Bei diesem Unternehmen handelt es sich um einen Dienstleister in der NoSQL- und Big Data-Branche. Die Plattform bietet eine Rangliste an, auf der verbreitete Datenbank-Engines aufzufinden sind.[98]

Diese Engines werden durch folgende Parameter mit Punkten bewertet:[99]

- **„Anzahl der Nennungen des Systems auf Websites“**: Die Messung für diesen Parameter erfolgt durch die Anzahl der Treffer in verschiedenen, verbreiteten Suchmaschinen.
- **„Allgemeines Interesse an dem System“:** Häufigkeit der Suche nach dem jeweiligen Datenbanksystem in Google Trends.

[97] Vgl. Metzger, S. 54
[98] Vgl. DB Engines (o. J.)
[99] Vgl. DB Engines (o. J.)

- **„Häufigkeit von technischen Diskussionen über das System“:** Anzahl von Diskussionen, Fragen und Antworten auf renommierten IT-Plattformen.
- **„Anzahl an Job-Angeboten, in denen das System genannt wird“**
- **„Anzahl an Profilen in professionellen Netzwerken, in denen das System aufgeführt wird“**

Die im Ranking am besten abschneidende, nicht-relationale Datenbank-Engine ist das dokumentenorientierte MongoDB. Diese Engine wird, wie bereits erwähnt, von verschiedenen Providern innerhalb der Services angeboten. Zu diesen zählen neben dem besonders bedeutenden Windows Azure-Service von Microsoft unter anderem MongoHQ und ObjectRocket. Als weitere erwähnenswerte Datenbank-Engine ist die vom Versandhändler Amazon.com entwickelte DynamoDB. Diese wird innerhalb der unternehmenseigenen Cloud-Computing-Plattform Amazon Web Services (AWS) angeboten. Amazon zählt neben Microsoft und Google zu den Pionieren im NoSQL-Datenbank-Bereich.[100]

Aus diesen Gründen wurden für den praktischen Teil dieser Arbeit die Dienste folgender Provider beansprucht:

- ObjectRocket (MongoDB)
- MongoHQ (MongoDB)
- Microsoft Windows Azure (MongoDB)
- Amazon WebServices (DynamoDB)

Diese werden im Folgenden anhand ihrer aussagekräftigsten Eigenschaften kurz vorgestellt. Im Anhang ist eine ausführliche Präsentation der Dienste zu finden, welche anhand von Screenshots unterstützt wird.

4.1 Object Rocket

Der Provider ObjectRocket bietet innerhalb seiner Dienste die Datenbank MongoDB an. Die Plattform ist über den Internet-Link *http://www.objectrocket.com* zu erreichen. Der Nutzer kann über die Weboberfläche im Browser Instanzen oder Datenbanken

[100] Vgl. DB Engines (o. J.)

anlegen. Um die Datenbank mit Massendaten zu füllen, empfiehlt sich jedoch die Verwendung einer Kommandozeile (auch „Konsole“ genannt), welche in herkömmlichen Betriebssystemen bereits standardmäßig implementiert ist (Windows: cmd, Linux/Mac OS X: Terminal). Für die Verbindung zum MongoDB-System muss dazu ein Treiberpaket heruntergeladen werden. Dieses Paket ist für die Verbindung zu allen Providern, welche MongoDB nutzen, geeignet.

Um eine Verbindung aufzubauen, sind standardisierte Kommandos in die Konsole einzutragen. Diese orientieren sich an der herkömmlichen Notation für MongoDB, welche wie folgt aufgebaut ist (Eingabe jeweils ohne </>).

```
<Befehlsname> <Webadresse des Providers>:<Port>/<Datenbank-Name> -u <Username> -p <Passwort>
```

Tabelle 2: MongoDB-Notation für den Verbindungsaufbau über eine Konsole

Abhängig von der gewünschten Aktion, die getätigt werden muss, wird an der Stelle <Befehlsname> der entsprechende Treiber eingegeben. Für sämtliche Interaktionen existieren jeweils unterschiedliche Treiber. Einige der verfügbaren Aktionen werden im folgenden Teil aufgelistet.

Befehlsname	Beschreibung
`./mongo`	Verbindung zur Datenbank-Konsole, einfacher Login u.a. um Datensätze einzufügen
`./mongodump`	Backup aus Datenbank erstellen
`./mongoimport`	Import aus JavaScript Object Notation (JSON), oder Comma-separated values (CSV)
`./mongorestore`	Datenbestand aus Backup importieren, welches über mongodump erstellt wurde (speziell als Backup gesichert)

Tabelle 3: Befehlsnamen aus dem MongoDB-Treiberpaket

4.1.1 Verbindung zur Datenbank und Aufruf des Dienstes

Über die Weboberfläche kann eingesehen werden, welche Datenbanken sich auf der persönlichen Plattform des Anwenders befinden. Um Datensätze einzufügen und um den vollen Funktionsumfang von MongoDB nutzen zu können, ist ein Login über die Konsole notwendig. Dazu ist die Navigation zum lokalen Verzeichnis, in dem sich die MongoDB-Treiber befinden, vorzunehmen. Dies geschieht jeweils über den Kurzbefehl „cd“ (change directory, englisch für „Verzeichnis wechseln“, gilt für Windows und Unix-Betriebssysteme). Die Verbindung wird im Fall von ObjectRocket über folgenden Befehl aufgebaut:

```
./mongo iad-c11-1.objectrocket.com:48035/TestDB
```

Tabelle 4: Kommando zum Verbindungsaufbau zu ObjectRocket

Die Webadresse und der Port sind jeweils beim Provider erhältlich.

Anzumerken ist, dass die „./“-Notation vor dem Befehlsname eine Unix-eigene Schreibweise darstellt. Diese Schreibweise findet hier Verwendung, da die Forschungen innerhalb dieser Ausarbeitung mittels Mac OS X 10.9 durchgeführt wurden. Auf Windows-Plattformen kann auf „./“ verzichtet werden.

4.1.2 Erstellung einer Datenbank

Eine Datenbank ist innerhalb des Webinterfaces von ObjectRocket anzulegen.

Nachdem diese erstellt wurde, muss eine Verbindung über die Kommandozeile hergestellt werden (siehe „Verbindung zur Datenbank/Aufruf des Diensts“). Nach erfolgreicher Verbindung und Login kann über folgenden Befehl eine neue Collection erstellt werden:

```
„db.createCollection('<Name der Collection>')“
```

Tabelle 5: Erstellen einer Collection in ObjectRocket

4.1.3 Daten ablegen

Um einzelne Datensätze abzulegen wird in der über den Befehl „./mongo“ aufgerufene Oberfläche folgender Befehl eingegeben:

```
„db.<Name der Collection>.insert({vorname: „Vorname“, nachname: „Nachname“, alter: Alter})“
```

Tabelle 6: Anlegen eines Datensatzes in ObjectRocket

Bei zahlreichen Datensätzen kann die wiederholte Eingabe des Befehls sehr mühsam sein. Sofern bereits Datensätze in einer kompatiblen Datei vorhanden sind, können diese „auf einmal“ importiert werden.

```
./mongoimport -h iad-c11-1.objectrocket.com:48035 -d <Name der Collection> -u <Username> -p <Passwort> --type <Dateityp> --file <Dateiname> --headerline
```

Tabelle 7: Import von mehreren Datensätzen in ObjectRocket

Zulässig für den Import von Massendaten sind die Dateitypen .csv, .json und .tsv. Unter Annahme, dass eine .csv-Datei importiert wird, ändert sich der Befehl wie folgt:

```
[...]--type csv --file testdata.csv[...]
```

Tabelle 8: Spezifizierung eines Imports von Massendaten mittels des Dateityps

4.1.4 Weitere Möglichkeiten innerhalb ObjectRocket:

Befehl	Beschreibung
db.<Name der Collection>.drop()	Collection löschen (Verbindung über ./mongo muss bestehen)
./mongodump -h iad-c11-1.objectrocket.com:48035/TestDB -u <Username> -p <Passwort> -o <Backup-Verzeichnis>	Über den Befehl ./mongodump wird ein Backup von der kompletten Datenbank auf dem lokalen Laufwerk (in der Regel das identische Verzeichnis, in dem sich die Datei ./mongodump befindet) abge-

	legt
./mongorestore -h iad-c11-1.objectrocket.com:48035 -d <Name der Collection> -u <User-name> -p <Passwort> <Backup-Verzeichnis>/<Name der gesi-cherten Datenbank>	Mittels des Befehls ./mongorestore kann eine Backup-Datei in die Daten-bank importiert werden

Tabelle 9: Ergänzende Kommados zu ObjectRocket

4.1.5 Kosten

Bei ObjectRocket kann zu Testzwecken ein 30-tägiger, kostenfreier Zugang angemeldet werden. Nach Ablauf der 30 Tagen wird automatisch auf den „Small"-Service (siehe Abbildung 21) umgeschaltet, sofern keine Kündigung eintrifft. Diese kann direkt über das Webportal in Form einer Service-Nachricht erfolgen. Die Preise für die unterschiedlichen Ressourcenmengen sind der folgenden Abbildung zu entnehmen.

Abb. 21: Tarifierung von ObjectRocket[101]

4.1.6 Service

ObjectRocket stellt folgende Zusatzdienstleistungen zur Verfügung:

- tägliche Backups
- durchgehendes Monitoring[102]

[101] Enthalten in: ObjectRocket (o. J.)
[102] Vgl. ObjectRocket (o. J.)

4.2 MongoHQ

Da es sich bei MongoHQ analog zu ObjectRocket um MongoDB handelt, sind die in der Tabelle beschriebenen Befehle nahezu identisch. Aus diesem Grund wird auf diese Grundlagen im folgenden Teil nicht mehr eingegangen.

Der Provider MongoHQ ist über den Hyperlink http://www.mongohq.com zu finden. Er bietet dem Kunden die Möglichkeit Datenbanken und Collections über die grafische Nutzeroberfläche im Browser zu erstellen. Weitere Funktionen, wie das Erstellen oder Importieren von Datensätzen, werden im folgenden Teil in Bezugnahme zu MongoHQ erläutert.

4.2.1 Verbindung zur Datenbank und Aufruf des Diensts

Die Verbindung zur MongoHQ-Datenbank unterscheidet sich zur ObjectRocket-Datenbank lediglich im verwendeten Hyperlink und dem erforderlichen Port, da auf eine standardisierte Notation zurückgegriffen wird.

Bei MongoHQ ist zunächst in der Weboberfläche eine Datenbank anzulegen. Bei der Erstellung einer Datenbank kann der Nutzer zwischen verschiedenen Tarifprofilen wählen, welche später Erwähnung finden.

```
./mongo paulo.mongohq.com:10090/<Name der Datenbank> -u
<Username> -p <Passwort>
```

Tabelle 10: Kommando zum Verbindungsaufbau zu MongoHQ

Nach erfolgreichem Login in die Datenbank kann über folgendes Kommando eine neue Collection in der erstellten Datenbank angelegt werden.

```
„db.createCollection(’<Name der Collection>’)“
```

Tabelle 11: Anlegen einer Collection in MongoHQ

Die angelegte Collection ist mittels dieser Eingabe mit einzelnen Datensätzen zu befüllen.

```
„db.<Name der Collection>.insert({vorname: „Vorname“, nachname: „Nachname“, alter: Alter})“
```

Tabelle 12: Einfügen eines Datensatzes in MongoHQ

Um mehrere Datensätze durch eine einzelne Eingabe zu importieren, wird in MongoHQ folgende Textzeile benötigt.

```
mongoimport -h paulo.mongohq.com:10090/TestDB -c <Name der Collection> -u <Username> -p <Passwort> --type csv --file testdata.csv --headerline
```

Tabelle 13: Import von mehreren Datensätzen in MongoHQ

In diesem Fall wurde analog zum ObjectRocket-Beispiel von einer vorhandenen .csv-Datei ausgegangen, welche nun importiert wird.

4.2.2 Weitere Möglichkeiten innerhalb MongoHQ

Befehl	Beschreibung
db.<Name der Collection>.drop()	Collection löschen (Verbindung über ./mongo muss bestehen)
./mongodump -h paulo.mongohq.com:10090/<Name der Datenbank> -u <Username> -p <Passwort> -o <Backup-Verzeichnis>	Über den Befehl ./mongodump wird ein Backup von der kompletten Datenbank auf dem lokalen Laufwerk (in der Regel das identische Verzeichnis, in dem sich die Datei ./mongodump befindet) abgelegt
./mongorestore -h paulo.mongohq.com:10090 -d <Name der Collection> -u <Username> -p <Passwort> <Backup-Verzeichnis>/<Name der gesicherten Datenbank>	Mittels des Befehls ./mongorestore kann eine Backup-Datei in die Datenbank importiert werden

Tabelle 14: Ergänzende Kommandos für MongoHQ

4.2.3 Kosten

	Speicher	**Kosten/Monat**	**Typ**
Sandbox	512 MB	Kostenlos	Prototyp-Plattform
Small	2 GB	$15	Single Server
Large	5 GB	$49	Single Server
	Kosten/Monat	**Wachstum**	**Typ**
4 GB	$100	$25/GB über 4GB	Replica Set
25 GB	$500	$20/GB über 25GB	Replica Set

Tabelle 15: Tarifierung von MongoHQ[103]

MongoHQ bietet zu Testzwecken einen 512MB große MongoDB-Service an (siehe Tabelle 15). Dieser ist in seiner Laufzeit nicht begrenzt. Der Kunde kann zudem wählen, auf welchen Servern seine Daten gespeichert werden sollen (z.B. Dallas, USA-East). Standardmäßig bietet MongoHQ „Single Server“ an. Dadurch werden die sich in der Datenbank befindenden Daten einfach gehalten. Diese Lösungen sind weder hochverfügbar noch zusätzlich gesichert. Der Ausfall eines Servers kann somit die Verfügbarkeit des Dienstes einschränken, im Extremfall sogar Datenverlust mit sich ziehen. Der redundant ausgelegte Typ „Replica Set“ ist demnach sicherheitstechnisch höher einzuordnen. Zudem ist dieser für Unternehmen empfehlenswert, die auf eine durchgängige Erreichbarkeit Wert legen.[104]

4.2.4 Service

MongoHQ bietet innerhalb seiner Provider-Dienstleistungen folgende Zusatzleistungen an:[105]

- Service per E-Mail in verschiedenen Sprachen
- Hohe Datensicherheit durch Backups (sofern gebucht)
- Durchgehendes Monitoring

[103] Enthalten in: MongoHQ (o. J.)
[104] Vgl. MongoHQ (o. J.)
[105] Vgl. MongoHQ (o. J.)

4.3 Microsoft Windows Azure

Sogar der weltweit größte Software-Anbieter Microsoft kommt nicht am Trend des Cloud-Computing vorbei. Mit der Windows Azure Plattform fasste das US-Amerikanische Unternehmen Fuß in dieser Sparte. Über einen integrierten Store stellt Microsoft eine große Auswahl an unterschiedlichen Diensten zur Verfügung und kann damit jeglichen Anforderungen der verschiedensten Endnutzer gerecht werden. Von SQL-Datenbanken und NoSQL-Datenbanken über Entwicklungsumgebungen bietet Microsoft ein breites Spektrum an. Damit lässt sich Azure dem Cloud-Computing Modell PaaS zuordnen (siehe Abbildung 22). Die Plattform ist mit dem Internet-Link *http://www.windowsazure.com* erreichbar. In Kooperation mit Mongolab bietet Microsoft MongoDB als NoSQL Cloud Dienst an.

Abb. 22: Bestandteile der Windows Azure Plattform[106]

Verbindung zur Datenbank/Aufruf des Diensts

Analog zu den meisten anderen MongoDB Anbietern kann über die Kommandozeile eine Verbindung zu der Datenbank aufgebaut werden. Der Port ist dabei nicht allgemeingültig, sondern wird mit jedem neuen Account individuell erstellt, wie in Abbildung 23 zu sehen ist.

[106] Enthalten in: Business-Cloud.de (2010)

To connect using the shell:

```
% mongo ds030607.mongolab.com:30607/MongoLab-u -u <dbuser> -p <dbpassword>
```

To connect using the shell:

```
% mongo ds030817.mongolab.com:30817/TestDB -u <dbuser> -p <dbpassword>
```

Abb. 23: Unterschiedliche Ports von Accounts bei demselben Cloud-Provider[107]

Im Gegensatz zu den anderen betrachteten MongoDB-Providern, liefert MongoLab eine Weboberfläche zur vollständigen Verwaltung der Datenbank. Diese erlaubt das anlegen, bearbeiten und löschen von Tabellen, Backups und einzelnen Datensätzen. Zudem lässt sich die Ansicht der Dokumente definieren, sodass eine bessere Übersichtlichkeit der Datensätze gegeben ist.

Define a table view for this collection ×

```
{
    "_id": "id"
}
```

You can view your documents in table format by defining a View for this collection. Views describe how to turn each JSON document (with potentially nested field values) into a flat set of fields for display as a row in a table.

To illustrate, let's say we have a collection with documents that look like this:

```
{ "firstName" : "Bob",
  "lastName" : "Smith",
  "address" : {
      "street" : "2447 Mt Royal Rd",
      "city" : "Pittsburgh",
      "state" : "PA",
      "zip" : "15217" } }
```

If you define a a View like this:

```
{ "Last Name" : "lastName",
  "City" : "address.city",
  "State" : "address.state" }
```

... you will get a table view like this:

Last Name	City	State
Smith	Pittsburgh	PA
Jones	Scarsdale	NY

Cancel Submit

Abb. 24: Erstellung von Schemas zur Anzeige von Dokumenten in Windows Azure[108]

[107] Enthalten in: Mongolab (2014)
[108] Enthalten in: Mongolab (2014)

Bei MongoLab kann zu Testzwecken eine sogenannte „Sandbox“ erstellt werden. Damit erhält der Nutzer eine Testumgebung mit einem maximalen Speicherverbrauch von 500 Megabyte. Die in der obigen Abbildung dargestellten Preise gelten für alle Kooperationspartner von MongoLab. Zusätzlich sind auch Partnerspezifische Preispläne vorhanden. Für jeden User steht der Standard-Email Support für alle Probleme zur Verfügung. Überdies ist auch ein kostenpflichtiger Premium Support erhältlich. Dieser beinhaltet einen 24x7 verfügbaren Notfallsupport, zur umgehenden Gewährleistung von Unterstützung im Problemfall.

Shared plans

Available in select datacenters at Amazon, Google, Joyent, Rackspace and Windows Azure

	Sandbox	Single-node	Cluster
included usable storage †	0.5 GB	2 GB	2 GB
available nodes (view details)	1 node	1 node	2 nodes
monthly base price	FREE	$15	$89
monthly extra storage charge ‡	n/a	$5 / GB	$5 / GB / node
maximum usable storage	0.5 GB	8 GB	8 GB

Abb. 25: Tarfifierung des MongoDB Dienstes von Mongolab[109]

4.4 Amazon Web Services

Der online Händler Amazon gehört neben Google zu den marktführenden Unternehmen im Cloud-Computing Bereich. Die Cloud Plattform Amazon Web Services (AWS) des US-amerikanischen Unternehmens stellt eine Vielzahl an Angeboten bereit, die sich ständig verändern und erweitern. In diesen Services sind daher inzwischen alle Vertreter der Geschäftsmodelle des Cloud-Computings vertreten. Aufgrund der Unwichtigkeit der meisten Angebote von AWS wird im Folgenden ein Einblick in die für die Arbeit relevanten Dienste gegeben.

[109] Enthalten in: Mongolab (2014)

Amazon Web Services

Compute & Networking
Direct Connect
Dedicated Network Connection to AWS
EC2
Virtual Servers in the Cloud
Route 53
Scalable Domain Name System
VPC
Isolated Cloud Resources

Storage & Content Delivery
CloudFront
Global Content Delivery Network
Glacier
Archive Storage in the Cloud
S3
Scalable Storage in the Cloud
Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage

Database
DynamoDB
Predictable and Scalable NoSQL Data Store
ElastiCache
In-Memory Cache
RDS
Managed Relational Database Service
Redshift
Managed Petabyte-Scale Data Warehouse Service

Deployment & Management
CloudFormation
Templated AWS Resource Creation
CloudTrail
User Activity and Change Tracking
CloudWatch
Resource and Application Monitoring
Elastic Beanstalk
AWS Application Container
IAM
Secure AWS Access Control
OpsWorks
DevOps Application Management Service

Analytics
Data Pipeline
Orchestration for Data-Driven Workflows
Elastic MapReduce
Managed Hadoop Framework
Kinesis
Real-time Processing of Streaming Big Data

App Services
CloudSearch
Managed Search Service
Elastic Transcoder
Easy-to-use Scalable Media Transcoding
SES
Email Sending Service
SNS
Push Notification Service
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components

Abb. 26: Überblick der Angebote von AWS[110]

4.4.1 Amazon Elastic Cloud Computing

Die Elastic Cloud Computing (EC2) bildet das Kernstück von AWS. Dem Endanwender wird dabei eine dynamische Rechnerarchitektur zur Verfügung gestellt, deren Ressourcen jederzeit nach Bedarf angepasst werden können. Bei EC2 handelt es sich um ein Hosting Dienst von Amazon, mit dem der Nutzer einen virtuellen Server einrichten und dauerhaft betreiben kann. Dementsprechend ist EC2 dem Cloud-Computing Modell IaaS zuzuordnen. Die Erstellung eines virtuellen Servers gestaltet sich durch die sogenannten Amazon Machine Images (AMI) als sehr einfach. Die AMIs sind von Amazon vorgefertigte Images von Betriebssystemen. Der Endanwender kann mit deren Hilfe diverse Linux Distributionen oder Microsoft Betriebssysteme auswählen. Wahlweise können auch Images von Drittanbietern verwendet oder auch eigene Betriebssystem-Abbilder erstellt werden. Die Konfiguration und Kontrolle des EC2 Dienstes vollständig über die Weboberfläche von AWS möglich. Dort lassen sich auch die erstellten Instanzen Starten, Herunterfahren und Löschen. Nachdem Start einer Instanz stehen dem Endanwender alle Möglichkeiten zur Verfügung, denn für den Inhalt ist jeder selbst verantwortlich. Der Dienst kann zur Erstellung von Ser-

[110] Enthalten in: AWS (2013a)

vices, welche nicht im Angebot von AWS enthalten sind, genutzt werden, wie beispielsweise zum Hosten von diversen NoSQL-Datenbanksystemen.[111]

4.4.2 Amazon DynamoDB

DynamoDB ist ein von der Plattform AWS bereitgestelltes NoSQL-Datenbanksystem. Analog zu den anderen Diensten von AWS lässt sich das Anlegen, Beseitigen und Konfigurieren der Datenbank und Datensätze vollständig über die Weboberfläche bewerkstelligen. DynamoDB ist der Gattung der Key-Value Datenbanken zuzuordnen und besitzt bis auf die Key-Value Zuordnung kein festes Schema. Daher können die Datensätze einer Tabelle eine unterschiedliche Anzahl von Attributen besitzen. Diese Attribute können zusätzlich von einem anderen Datentyp sein. DynamoDB unterstützt dabei die von relationalen Datenbanken bekannten Datentypen Zahlen, Zeichenfolgen und Binärdaten.[112]

Abb. 27: Erstellen einer DynamoDB Instanz in AWS[113]

[111] Vgl. Baun, C./u. a. (2011), S.46
[112] Vgl. AWS (2013b)
[113] Enthalten in: AWS (2013a)

Abbildung 27 stellt die Erstellung einer Datenbank über die AWS Management Console dar. Der Nutzer wird dabei in fünf Schritten durch eine Startkonfiguration für die Datenbank geführt. Während dieser Konfiguration muss der Endanwender den Primärschlüssel und den Datendurchsatz festlegen, dieser kann wiederum nachträglich an den Bedarf angepasst werden. Wahlweise besteht die Möglichkeit einen Index und einen Benachrichtigungsdienst einzurichten. Innerhalb weniger Minuten ist der Auftrag abgeschlossen und die Datenbank verfügbar. Ferner kann der Dienst DynamoDB durch zusätzliche Anwendungen erweitert werden. Mit einer Integeration des Dienstes Amazon Elasitc Map Reduction (EMR), basierend auf das von Google entwickelte Hadoop Framework, ist eine Analyse großer Datensätze innerhalb DynamoDB möglich. Die Ergebnisse der Analyse können wiederum in zusätzlichen Diensten archiviert werden. AWS stellt seinen Kunden damit eine nahtlose Kombination vieler Anwendungen zur Verfügung.[114]

[114] Vgl. AWS (2013b)

5 Fazit

Teil dieser Ausarbeitung war es, die theoretischen Grundlagen zum Thema NoSQL-Datenbanksysteme zu erläutern. Dabei wurde insbesondere auf die Verwendung von MongoDB in Verbindung mit Cloud-Diensten eingegangen. Hierbei wurden verschiedene Interaktionen mit MongoDB erläutert. Einzelne Interaktionen wurden sowohl über die Kommandozeile des Clients, als auch über das Web-Interface des jeweiligen Cloud-Providers durchgeführt. Die Ausarbeitung dokumentiert dabei das Verbinden mit MongoDB, das Anlegen einzelner Datenbanken und das Transferieren bzw. das Administrieren von Daten. Bezüglich MongoDB wurden die Cloud-Provider ObjectRocket, MongoHQ und Windows Azure betrachtet. Zudem wurde auf DynamoDB in Verbindung mit AWS eingegangen.

Diese Ausarbeitung liefert somit einen ersten Überblick über die theoretischen Grundlagen, Konzepte und Möglichkeiten von NoSQL-Datenbanksystemen, sowie über ihren cloudbezogenen Einsatz. Für die einzelnen NoSQL-Cloud-Dienste wurden jeweils ihre Lizensierungsmodelle inkl. der anfallenden Kosten hervorgehoben. Die Arbeit richtet sich vor allem an Unternehmen, die den Einsatz von NoSQL-Datenbanksystemen erwägen und soll diese gleichzeitig ermutigen, sich mit dem Thema auseinanderzusetzen. Vor allem im Zeitalter von Big-Data ist das Thema nicht zu vernachlässigen, weshalb NoSQL-Datenbanksysteme ihre Daseinsberechtigung (neben den relationalen Datenbanken) besitzen. Gerade aktuelle Themen und Entwicklungen aus der IT-Branche wie bspw. Semantic Web oder die In-Memory-Datenhaltung lassen nur erahnen, welchen Stellenwert NoSQL-Datenbanksysteme in der Zukunft haben könnten. Ob sich eine NoSQL-Datenbank aus der Cloud für ein Unternehmen eignet, muss jedoch fallspezifisch geprüft werden. Besonders ist hierbei anzumerken, dass NoSQL-Datenbanksysteme nicht pauschal als Ersatz für relationale Datenbanksysteme zu verstehen sind.

6 Anhang

Anhangsverzeichnis

Anhang 1: MongoHQ – Login in die Web-Plattform

Der Nutzer des Dienstes MongoHQ hat sich mit seiner registrierten E-Mail-Adresse und des Passworts auf der Plattform einzuloggen.

Anhang 2: MongoHQ – Öffnen einer Datenbank

Nach dem Login ist eine Übersicht über die bereits vorhandenen Datenbanken zu sehen. Klickt der Nutzer auf die bestehende Datenbank - in diesem Falle „Cobain“ - gelangt er zur detaillierten Ansicht.

Anhang 3: MongoHQ – Übersicht über die Collections in einer DB

In der erstellten Datenbank „Cobain“ befinden sich derzeit keine Collections.

Anhang 4: MongoHQ – Anlegen einer Collection

Um eine neue Collection anzulegen, muss der Nutzer auf „Create a collection“ klicken. Daraufhin öffnet sich ein weiteres Feld, wo der Name der neuen Collection einzutragen ist.

Anhang 5: MongoHQ – Anzeige einer angelegten Collection

Die neu erstelle Collection wird daraufhin im Menü angezeigt.

Anhang 6: MongoHQ – Ansicht der Administrations-Oberfläche

Beim Klicken auf das Feld „Admin“ bekommt der Kunde unter anderem eine Übersicht über die Auslastung des verwendeten Systems geboten. Des Weiteren sind hier die für die Konsole erforderlichen Kommandos teilweise zu entnehmen.

Anhang 7: MongoHQ – Erstellen einer neuen Datenbank

Durch den Klick auf „Add Database“ (deutsch: Datenbank hinzufügen) im Startmenü kann eine weitere Datenbank erstellt werden. Der Kunde kann dabei zwischen den verschiedenen Datenbank-Typen wählen. Diese weisen jeweils eine unterschiedliche Tarifierung auf. Für die Testzwecke innerhalb dieses Projekts wurde die „Sandbox“-Lösung gewählt. Diese Lösung ist nicht redundant ausgelegt. Wird dies gewünscht, hat der Kunde die Option „Replica Set“ zu wählen.

Anhang 8: MongoHQ – Bestätigung bei einer erfolgreichen Datenbank-Erstellung

Nach erfolgreicher Anlegung der neuen Datenbank wird dem Kunden eine Meldung übermittelt, dass der Vorgang abgeschlossen wurde.

Anhang 9: ObjectRocket – Login in die Web-Plattform

Beim Aufruf von „https://app.objectrocket.com“ wird dem Kunden das Login-Menü für die Plattform angezeigt. In die entsprechenden Felder sind die jeweiligen Anmeldedaten einzugeben, worauf ein Login erfolgt.

Anhang 10: ObjectRocket – Anlegen einer Instanz

Im Startmenü, welches nach dem Login erscheint, kann der Kunde eine Instanz erstellen. In diesen Instanzen können mehrere Datenbanken angelegt werden. Der Kunde kann beim Erstellen eine gewünschte Datenbankgröße sowie die Zone, in der sich die Server befinden, auswählen.

Anhang 11: ObjectRocket – Anzeige von Daten über die erstellte Instanz

Nachdem die Instanz erstellt wurde kann der Kunde diverse Informationen über diese einholen. Dazu zählen unter anderem die verwendete MongoDB-Version, die Auslastung, sowie Verbindungsdaten.

Anhang 12: ObjectRocket – Aufruf der erstellten Instanz

Beim Klick auf „Instance Details“ beim Instanzname „YOLO“ kann der Kunde die Seite mit den sich in „YOLO“ befindenden Datenbanken aufrufen.

Anhang 13: ObjectRocket – Anzeige der erstellten Instanz

https app.objectrocket.com/instances/YOLO — ObjectRocket

ObjectRocket Dashboard Instances Messages Help DHBW-NOSQL [Sign Out]

My Instances / YOLO :48035

Databases ACL Backups Settings

Add Database Copy Remote Database

Name	Objects	Avg Object Size	Data Size	Indexes	Index Size	Storage Size	File Size	Action
Hendrix	8	71 Bytes	568 Bytes	2	16.4 kB	20.5 kB	209.7 MB	

Showing 1 to 1 of 1 entries
10 records per page ← Previous 1 Next →

050282bbbb8dc47827a4dee1d5b475b8dbc7ee64
© ObjectRocket 2012

Die sich in „YOLO“ befindenden Datenbanken werden nun auf der Seite angezeigt. Neben der Bezeichnung „Hendrix“ erhält der Kunde Informationen über die Größe und die Anzahl der sich in der Datenbank befindenden Objekte.

Anhang 14: ObjectRocket – Konfiguration einer Access Control List

https app.objectrocket.com/instances/YOLO — ObjectRocket

ObjectRocket Dashboard Instances Messages Help DHBW-NOSQL [Sign Out]

My Instances / YOLO :48035

Databases ACL Backups Settings

Add ACL

	Source IP CIDR	Action	Description
Delete	0.0.0.0/1	Allow	Allow Any
Delete	128.0.0.0/1	Allow	Allow Any

Showing 1 to 2 of 2 entries
10 records per page ← Previous 1 Next →

050282bbbb8dc47827a4dee1d5b475b8dbc7ee64
© ObjectRocket 2012

Mittels einer Access Control List (ACL) können Zugriffsberechtigungen für bestimmte Internet Protocol (IP)-Adressen definiert werden.

Anhang 15: Windows Azure – Erstellung und Anmeldung eines Accounts

Über den Hyperlink *http://www.windowsazure.com* ist die Cloud Plattform von Microsoft zu erreichen. Die obigen Abbildungen zeigen den Prozess der Erstellung eines Accounts mit anschließender Anmeldung. Allerdings ist eine Microsoft E-Mailadresse für die Erstellung eines Accounts notwendig. Nach der Anmeldung wird der Nutzer auf die Verwaltungsoberfläche von Windows Azure weitergeleitet. (siehe Anhang 16)

www.windowsazure.com/en-us/account/?fb=de-de – Windows Azure Accounts | Windows Azure

Nagios Cluster einrichten – Linux – Monitoring-Portal

Windows Azure Accounts | Windows Azure

SALES: 0800-180-8941 | ACCOUNT | PORTAL

Windows Azure

SOLUTIONS PRICING DOCUMENTATION DOWNLOADS ADD-ONS COMMUNITY SUPPORT

FREE TRIAL

Dieser Inhalt ist derzeit nur in englischer Sprache verfügbar. Wir entschuldigen uns für die Unannehmlichkeiten.

Welcome to Windows Azure

Get started

Get started with a free Windows Azure trial today

Get a free account

Manage

Configure and use Windows Azure services

Management Portal

Track Usage

Track your Windows Azure usage and subscriptions

Account Management

Go Social Windows Azure Community Account

Microsoft Corporation login.microsoftonline.com/login.srf?wa=wsignin1.0&wtrealm=https%3a%2f%2flogin.windows.net%2f&wreply=https%3a%2f%2flogin.windows.net

Cloud-Optimierung für Ihr Unternehmen

Windows Azure

Geben Sie die E-Mail-Adresse des Kontos ein, mit dem Sie sich anmelden möchten.

jemand@example.com

Weiter Abbrechen

Hier funktionierende Organisationskonten können überall dort verwendet werden, wo dieses Symbol angezeigt wird.

© 2013 Microsoft Rechtliche Hinweise Datenschutzbestimmungen

Feedback senden

Microsoft Corporation login.microsoftonline.com/login.srf?wa=wsignin1.0&wtrealm=https%3a%2f%2flogin.windows.net%2f&wreply=https%3a%2f%2flogin.windows.net
Cloud-Optimierung für Ihr Unternehmen
Windows Azure
dhbw.nosql@outlook.com
(Microsoft-Konto)
Umleitung
Sie werden auf die Anmeldeseite für Ihr Microsoft-Konto umgeleitet. Abbrechen
Angemeldet bleiben
Dieses Konto vergessen
Hier funktionierende Organisationskonten können überall dort verwendet werden, wo dieses Symbol angezeigt wird.
© 2013 Microsoft Rechtliche Hinweise Datenschutzbestimmungen
Feedback senden

Microsoft Corporation login.live.com
Bei Windows Azure anmelden
Sie verfügen über kein Microsoft-Konto? Registrieren Sie sich jetzt.
Mit Ihrem Unternehmenskonto anmelden
Anmelden
Microsoft-Konto Was ist das?
dhbw.nosql@outlook.com
Angemeldet bleiben
Anmelden
Können Sie nicht auf Ihr Konto zugreifen?
Melden Sie sich mit einem Einmalcode an
Microsoft
©2013 Microsoft Nutzungsbedingungen Datenschutz und Cookies
Hilfecenter Feedback

Anhang 16: Windows Azure – Anlegen einer Datenbank

Nach der Anmeldung auf der Benutzeroberfläche von Windows Azure befindet sich der Nutzer im Reiter „Alle Elemente“. Mittels einem Mausklick auf den Menüpunkt „Neu“ (1) wird ein Untermenü aufgeklappt. Über dieses Untermenü kann der Windows Azure Store geöffnet werden (2). Im Store angekommen kann der Endanwender anhand einer Taskleiste durch alle offerierten Angebote, sogenannte „Add-Ons“, der Plattform scrollen (3). Mit einem Klick auf das gewünschte Angebot wird der Nutzer zur genauen Produktbeschreibung weitergeleitet. Im nächsten Schritt lässt sich das Add-On personalisieren. Dabei wählt der Kunde seinen Tarif (4) und vergibt dem Dienst einen Namen (5). Die Plattform weist jeweils unterschiedliche Tarife auf. Für die Testzwecke innerhalb dieses Projekts wurde die „Sandbox“-Lösung gewählt. Nach Abschluss der Transaktion ist im Startmenü der Plattform der aktuelle Status des Dienstes zu sehen (6). Sobald der Dienst bereit ist, kann dieser mittels einem Klick darauf, verwaltet werden (7).

IN STORE KAUFEN

Add-On auswählen

ALLE
APP-DIENSTE
DATEN

Logentries
Microsoft Translator
MongoDB - Preview
MongoLab
New Relic
Phone Number Validation

3

MongoLab
ObjectLabs Corporation

MongoLab is a fully-managed cloud database service featuring highly-available MongoDB databases, automated backups, web-based tools, 24/7 monitoring, and expert support. By hosting MongoDB on MongoLab's Database-as-a-Service (DBaaS) platform, developers and IT professionals are free to focus their attention on product development instead of operations.

VERÖFFENTLICHUNGSDATUM 2012

IN STORE KAUFEN

Add-On personalisieren

PLÄNE (2)

Sandbox
Our free sandbox plan is a great way to experience MongoDB on Windows Azure! It includes 0.5 GB of storage.
0 EUR/month

Shared Cluster
A highly-available MongoDB Replica Set cluster on shared Windows Azure hosts. This plan includes 8 GB of storage.

4

AKTIONSCODE

NAME
TestDB

5

REGION
Westliche USA

MongoLab
ObjectLabs Corporation

MongoLab is a fully-managed cloud database service featuring highly-available MongoDB databases, automated backups, web-based tools, 24/7 monitoring, and expert support. By hosting MongoDB on MongoLab's Database-as-a-Service (DBaaS) platform, developers and IT professionals are free to focus their attention on product development instead of operations.

VERÖFFENTLICHUNGSDATUM 2012

manage.windowsazure.com/%40dhbwnosqloutlook.onmicrosoft.com#Workspaces/StoreExtension/Store — Add-ons – Windows Azure

Windows Azure GUTHABENSTATUS dhbw.nosql@outlook.com

ALLE ELEMENTE
WEBSITES
VIRTUELLE COMPUTER
MOBILE DIENSTE
CLOUD-DIENSTE
SQL-DATENBANKEN
SPEICHER
HDINSIGHT
MEDIENDIENSTE
SERVICE BUS
VISUAL STUDIO ONLINE
BIZTALK-DIENSTE

add-ons VORSCHAU

NAME	TYP	STATUS	ANGEBOT	PLAN	ABONNEMENT
MongoLab	App-Dienst	Gestartet	MongoLab	Sandbox	Kostenlose Testversion
TestDB	App-Dienst	Wird erstellt...	MongoLab	Sandbox	Kostenlose Testversion

6

Kaufen von Add-On TestDB.

NEU VERWALTEN VERBINDUNGSINFORMATIONEN UPDATE KONTAKTEINSTELLUNGEN LÖSCHEN

manage.windowsazure.com/%40dhbwnosqloutlook.onmicrosoft.com#Workspaces/StoreExtension/DevService/TestDB/quickstart — Add-ons – Windows Azure

Windows Azure GUTHABENSTATUS dhbw.nosql@outlook.com

MongoLab
TestDB

testdb VORSCHAU

DASHBOARD

MongoLab is a fully-managed cloud database service featuring highly-available MongoDB databases, automated backups, web-based tools, 24/7 monitoring, and expert support. By hosting MongoDB on MongoLab's Database-as-a-Service (DBaaS) platform,

7

Add-On verwalten
Besuchen Sie die ObjectLabs Corporation-Website, um mehr über die nächsten Schritte zu erfahren.

Letzter Vorgang
Create - Succeeded

Webseite
Besuchen Sie die Webseite "ObjectLabs Corporation".

Kontakteinstellungen

NEU VERWALTEN VERBINDUNGSINFORMATIONEN UPDATE KONTAKTEINSTELLUNGEN LÖSCHEN

Anhang 17: Windows Azure – Erstellen einer Tabelle in Mongolab

Über die Verwaltungsfunktion der Windows Azure Plattform wird der User auf die Weboberfläche des Dienstes weitergeleitet. Nach der Weiterleitung ist eine Übersicht der erstellten Datenbank zu sehen. Der Name der Datenbank entspricht dabei dem Namen aus Windows Azure (1). Bis auf die vom System selbst erstellen Collections ist die Datenbank „TestDB“ noch leer. Um eine neue Collection anzulegen, muss der Nutzer auf „Add collection“ klicken. Daraufhin öffnet sich ein weiteres Feld, wo der Name der neuen Collection einzutragen ist (2).

Anhang 18: Windows Azure – Anlegen von Datensätzen in Mongolab via Webinterface

Mongolab liefert ein Webinterface zur vollständigen Verwaltung der Datenbank. Diese erlaubt das anlegen, bearbeiten und löschen von Tabellen, Backups und einzelner Datensätze. Über das Feld „Add“ kann ein neuer Datensatz angelegt werden (1). Der Kunde wird dabei zu einer webbasierten Kommandozeile weitergeleitet (2). Mit der entsprechenden Syntax können Datensätze angelegt werden. Innerhalb weniger Sekunden ist der neue Datensatz in der Collection vorhanden (3).

https mongolab.com/databases/TestDB/collections/DHBW-Test/_new?pageSize=10&pageNum=0&totalCount=1& — MongoLab: MongoDB-as-a-Service

mongolab

Docs & Support Account Log out

{ user: "young-oasis-1", account: "young-oasis-1" }

Home : { db : "TestDB", collection : "DHBW-Test" }

Create document / obj

2

{"Bandname": "Die Orsons"}

question ?

Cancel and go back | Create and go back | Create and continue editing

https mongolab.com/databases/TestDB/collections/DHBW-Test?saved=1387876872624&q=&s=&f=&pageNum=0&pageSize=10 — MongoLab: MongoDB-as-a-Service

mongolab

Docs & Support Account Log out

{ user: "young-oasis-1", account: "young-oasis-1" }

Home : { db : "TestDB" }

Collection: DHBW-Test (rename)

Documents | Indexes | Stats | Tools

Documents

Delete all | Add

--- Start new search ---

All Documents

Display mode: list table (edit table view)

widen column

records / page 10

[1 - 2 of 2]

```
{
    "_id": {
        "$oid": "52b951eae4b0a8d71f6ff905"
    },
    "Test": "Dies ist ein Testobjekt"
}
```

```
{
    "_id": {
        "$oid": "52b95208e4b0a8d71f6ff906"
    },
    "Bandname": "Die Orsons"
}
```

3

records / page 10

[1 - 2 of 2]

Documents (aka Objects)

From the "Documents" tab you can browse and search for objects in this collection. All standard query constructs are supported except for map/reduce queries. To use map/reduce, use the MongoDB shell (note that temporary result collections will be viewable in MongoLab).

You can also add, edit, and delete individual documents from here. Bulk collection updates are not yet supported in this UI (although they are supported in the shell).

question ?

Anhang 19: Windows Azure – Import von Datensätzen

In der Weboberfläche von Mongolab befindet sich eine Beschreibung für den Import bzw. Export von Daten. Im Wesentlichen werden die drei Dateitypen Binary, JSON und CSV von NoSQL-Datenbanken unterstützt. Die jeweilige Syntax des Import-/Exportbefehls lässt sich aus der Beschreibung entnehmen (1). Als Testzweck wurde eine Testdatei vom Typ CSV mit 90000 Objekten erstellt und diese dann in die Collection „DHBW-TEST“ der Mongolab Datenbank „TestDB“ importiert (2). Der Import und Export von Daten funktioniert ausschließlich über die Kommandozeile. Nach erfolgreichem Import lassen sich alle Datensätze einsehen (3).

```
[Wiederhergestellt]
Last login: Tue Dec 24 09:14:04 on console
Timms-MacBook-Pro:bin Timm$ ls -l
total 608208
drwxr-xr-x  3 Timm  staff       102 18 Dez 15:02 Backup
-rwxr-xr-x@ 1 Timm  staff  22503804 31 Okt 15:26 bsondump
-rwxr-xr-x@ 1 Timm  staff  12842856 31 Okt 15:26 mongo
-rwxr-xr-x@ 1 Timm  staff  22614596 31 Okt 15:26 mongod
-rwxr-xr-x@ 1 Timm  staff  22546400 31 Okt 15:26 mongodump
-rwxr-xr-x@ 1 Timm  staff  22511772 31 Okt 15:26 mongoexport
-rwxr-xr-x@ 1 Timm  staff  22538556 31 Okt 15:26 mongofiles
-rwxr-xr-x@ 1 Timm  staff  22536104 31 Okt 15:26 mongoimport
-rwxr-xr-x@ 1 Timm  staff  22503340 31 Okt 15:26 mongooplog
-rwxr-xr-x@ 1 Timm  staff  22504456 31 Okt 15:26 mongoperf
-rwxr-xr-x@ 1 Timm  staff  22549536 31 Okt 15:26 mongorestore
-rwxr-xr-x@ 1 Timm  staff  17725012 31 Okt 15:26 mongos
-rwxr-xr-x@ 1 Timm  staff  22502148 31 Okt 15:26 mongosniff
-rwxr-xr-x@ 1 Timm  staff  22577860 31 Okt 15:26 mongostat
-rwxr-xr-x@ 1 Timm  staff  22509628 31 Okt 15:26 mongotop
-rw-r--r--@ 1 Timm  staff   5880693  1 Jan  1970 testdata.csv
-rw-r--r--  1 Timm  staff   4521859  1 Jan  1970 testdata2.csv
drwxr-xr-x  3 Timm  staff       102 11 Dez 14:54 xtra
Timms-MacBook-Pro:bin Timm$ mongoimport -h ds030817.mongolab.com:30817 -d TestDB -c DHBW-Test -u Jagger -p mick --file testdata.csv --type csv --headerline
-bash: mongoimport: command not found
Timms-MacBook-Pro:bin Timm$ ./mongoimport -h ds030817.mongolab.com:30817 -d TestDB -c DHBW-Test -u Jagger -p mick --file testdata.csv --type csv --headerline
connected to: ds030817.mongolab.com:30817
Tue Dec 24 10:31:22.697           Progress: 6292/5880693  0%
Tue Dec 24 10:31:22.705                   100     25/second
Tue Dec 24 10:31:25.010           Progress: 399269/5880693       6%
Tue Dec 24 10:31:25.010                   6200    885/second
Tue Dec 24 10:31:28.003           Progress: 1279651/5880693      21%
Tue Dec 24 10:31:28.003                   19700   1970/second
Tue Dec 24 10:31:31.020           Progress: 2058628/5880693      35%
Tue Dec 24 10:31:31.020                   31600   2430/second
Tue Dec 24 10:31:34.002           Progress: 2806176/5880693      47%
Tue Dec 24 10:31:34.002                   43000   2687/second
Tue Dec 24 10:31:37.015           Progress: 3446720/5880693      58%
Tue Dec 24 10:31:37.015                   52800   2778/second
Tue Dec 24 10:31:40.011           Progress: 4212674/5880693      71%
Tue Dec 24 10:31:40.011                   64500   2931/second
Tue Dec 24 10:31:43.056           Progress: 5018437/5880693      85%
Tue Dec 24 10:31:43.056                   76800   3072/second
Tue Dec 24 10:31:46.007           Progress: 5867599/5880693      99%
Tue Dec [illegible]                       [illegible]   3207/second
Tue Dec 24 10:31:46.052 check 9 90001
Tue Dec 24 10:31:46.430 imported 90000 objects
```

2

https mongolab.com/databases/TestDB/collections/DHBW-Test — MongoLab: MongoDB-as-a-Service

```
},
"Herausgeber": "Xema",
"Nummer": "1234-5678-9012-3456",
"Deckung": 2000000

{
  "_id": {
    "$oid": "52b954672399a0dc7b6b817e"
  },
  "id": 1,
  "first_name": "Nancy",
  "last_name": "Jacobs"

{
  "_id": {
    "$oid": "52b954672399a0dc7b6b817f"
  },
  "id": 2,
  "first_name": "Jason",
  "last_name": "Patterson"

{
  "_id": {
    "$oid": "52b954672399a0dc7b6b8180"
  },
  "id": 3,
  "first_name": "Jerry",
  "last_name": "Mason"

{
  "_id": {
    "$oid": "52b954682399a0dc7b6b8181"
  },
  "id": 4,
  "first_name": "Christopher",
  "last_name": "Hall"

{
  "_id": {
    "$oid": "52b954682399a0dc7b6b8182"
  },
  "id": 5,
  "first_name": "Harold",
  "last_name": "Simmons"

{
  "_id": {
    "$oid": "52b954692399a0dc7b6b8183"
  },
  "id": 6,
  "first_name": "Walter",
  "last_name": "Diaz"
```

question ?

records / page 10

[1 - 10 of 90004] next > last >>

3

Anhang 20: Amazon Web Services Anmeldung

Mit dem Hyperlink *http://www.aws.amazon.com* gelangt der Kunde auf die Startseite des Cloud-Computing Geschäftsbereiches von Amazon. Mit einem Klick auf den „Anmelden"-Button (1), kann der Nutzer ein neues Konto registrieren oder mit seinem bereits registrierten Konto anmelden (2). Im Startmenü, welches nach erfolgreichem Login erscheint, kann der Kunde seinen Account verwalten. Über die AWS Management Console erreicht der Nutzer den AWS Store (3).

aws.amazon.com/de/ — Amazon Web Services (Deutsch)

amazon web services

1 Anmelden Konto / Konsole Deutsch

Produkte u. Lösungen AWS Product Information Entwickler Support

Vorstellung von Amazon AppStream

Streamen Sie Ihre ressourcenintensiven Anwendungen aus der AWS-Cloud.

Das dreiminütige Video ansehen »

Kostenloser Einstieg » Starten Sie virtuelle Maschinen und Anwendungen in Minuten.

Für Sie ausgewählte Links

Events	Neu hier?	Architekturen	Kontakt
Start Ups	Partner	Fallstudien	Whitepapers

https www.amazon.com/ap/signin?openid.assoc_handle=aws&openid.return_to=https%3A%2F%2Fportal.aws.amazon.com%2Fgp%2Faws%2Fdeveloper%2Fregistration%

amazon web services

Sign In or Create an AWS Account

You may sign in using your existing Amazon.com account or you can create a new account by selecting "I am a new user."

My e-mail address is:

I am a new user.

I am a returning user and my password is:

Sign in using our secure server

Forgot your password?

Has your e-mail address changed?

2

Learn more about AWS Identity and Access Management and AWS Multi-Factor Authentication, features that provide additional security for your AWS Account.

About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below.

https portal.aws.amazon.com/gp/aws/manageYourAccount — Amazon Web Services

amazon web services

Anmelden | Konto / Konsole | Deutsch

AWS Management Console

My Account

Billing & Cost Management

Security Credentials

3

Produkte u. Lösungen | AWS Product In... | ...upport

...ki | Abmelden

Kontonummer 0917-8951-4461

Konto

- Kontoaktivität
- AWS Identity and Access Management
- AWS Management Console
- Konsolidierte Fakturierung
- Reserved Instance Marketplace Setting
- DevPay
- **Verwalten Ihres Kontos**
- Zahlungsweise
- Persönliche Informationen
- Sicherheitsnachweise
- Nutzungsberichte
- Billing Alerts
- Billing Preferences

Verwalten Ihres Kontos

Dienstleistungen, für die Sie registriert sind

Amazon CloudFormation	Amazon Simple Queue Service (SQS)
Amazon CloudFront	Amazon Simple Storage Service (S3)
Amazon CloudSearch	Amazon Simple Workflow Service (SWF)
Amazon CloudWatch	Amazon SimpleDB
Amazon DynamoDB	Amazon Virtual Private Cloud (VPC)
Amazon Elastic Compute Cloud (EC2)	Auto Scaling
Amazon Elastic MapReduce	AWS CloudHSM
Amazon Elastic Transcoder	AWS Data Pipeline
Amazon ElastiCache	AWS Direct Connect
Amazon Glacier	AWS Elastic Beanstalk
Amazon Kinesis	AWS Import/Export
Amazon Mechanical Turk	AWS OpsWorks
Amazon Redshift	AWS Storage Gateway
Amazon Relational Database Service (RDS)	AWS Support (Basic)
Amazon Route 53	Elastic Block Store (EBS)
Amazon Simple Email Service (SES)	Elastic Load Balancing
Amazon Simple Notification Service (SNS)	Product Advertising API

Anhang 21: AWS – Überblick der Angebote

Der AWS Store bietet eine Vielzahl an Cloud Produkten, welche zur besseren Übersicht in bestimmte Kategorien unterteilt wurden. Im Rahmen der Forschungsarbeit wurde der Dienst DynamoDB in Anspruch genommen.

https console.aws.amazon.com/console/home?# — AWS Management Console
Reader
Services Edit Marcel Dittkowski Global Help

Amazon Web Services

Compute & Networking
Direct Connect
Dedicated Network Connection to AWS
EC2
Virtual Servers in the Cloud
Route 53
Scalable Domain Name System
VPC
Isolated Cloud Resources

Storage & Content Delivery
CloudFront
Global Content Delivery Network
Glacier
Archive Storage in the Cloud
S3
Scalable Storage in the Cloud
Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage

Database
DynamoDB
Predictable and Scalable NoSQL Data Store
ElastiCache
In-Memory Cache
RDS
Managed Relational Database Service
Redshift
Managed Petabyte-Scale Data Warehouse Service

Deployment & Management
CloudFormation
Templated AWS Resource Creation
CloudTrail
User Activity and Change Tracking
CloudWatch
Resource and Application Monitoring
Elastic Beanstalk
AWS Application Container
IAM
Secure AWS Access Control
OpsWorks
DevOps Application Management Service

Analytics
Data Pipeline
Orchestration for Data-Driven Workflows
Elastic MapReduce
Managed Hadoop Framework
Kinesis
Real-time Processing of Streaming Big Data

App Services
CloudSearch
Managed Search Service
Elastic Transcoder
Easy-to-use Scalable Media Transcoding
SES
Email Sending Service
SNS
Push Notification Service
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components

Additional Resources
Getting Started
See our documentation to get started and learn more about how to use our services.
Trusted Advisor
Best practice recommendations to save money, improve fault tolerance, increase performance, and close security gaps.

Service Health
Amazon Relational Database Service (Sao Paulo)
Additional Issues: 1
Updated: Dec 18 2013 15:45:00 GMT+0100
Service Health Dashboard

Set Start Page
Console Home

AWS Marketplace
Find & buy software, launch with 1-Click and pay by the hour.

 Privacy Policy Terms of Use Feedback

Anhang 22: AWS DynamoDB – Erstellen einer Datenbank

Die folgenden sechs Abbildungen zeigen das Erstellen einer Datenbank. Anmerkung: Der Kunde kann bei der Erstelung der Datenbank den Ort des Rechenzentrums auswählen. Dieser Aspekt spielt eine wichtige Rolle im Zusammenhang mit dem Datenschutz (1).

https console.aws.amazon.com/dynamodb/home?region=us-east-1#gs: — DynamoDB Management Console

Services Edit Marcel Dittkowski N. Virginia Help

Create Table Cancel

PRIMARY KEY — ADD INDEXES (optional) — PROVISIONED THROUGHPUT CAPACITY — THROUGHPUT ALARMS (optional) — SUMMARY

Add Indexes (optional)

An index is a data structure that maintains an alternate hash and range key. You can use it to Query an item the same way you use the table hash and range key.

Index Type:* Global Secondary Index

String Number Binary

Index Hash Key:*

String Number Binary

Index Range Key:

Index Name:*

Projected Attributes:* All Attributes

Add Index To Table

Table Indexes

Index Type	Index Hash Key	Index Range Key	Index Name	Projected Attributes
No Indexes exist. Enter values and click 'Add Index To Table' to create one.				

You can only define indexes at table creation time, and cannot remove or modify them later. Please see Secondary Indexes, Global Index Guidelines, and Local Index Guidelines for more information and other considerations.

Back Continue Help

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Feedback

https console.aws.amazon.com/dynamodb/home?region=us-east-1#gs: — DynamoDB Management Console

Services Edit Marcel Dittkowski N. Virginia Help

Create Table Cancel

PRIMARY KEY — ADD INDEXES (optional) — PROVISIONED THROUGHPUT CAPACITY — THROUGHPUT ALARMS (optional) — SUMMARY

Provisioned Throughput Capacity:

Help me calculate how much throughput capacity I need to provision

Throughput capacity to provision:

Amazon DynamoDB lets you specify how much read and write throughput capacity you wish to provision for your table. Using this information, Amazon will provision the appropriate resources to meet your throughput needs. More Information

Read Capacity Units: 10

Write Capacity Units: 5

Throughput capacity for this table will cost up to $2.91 per month if you have exceeded the free tier.

If you exceed the free tier you are cha[...] actively use your provisioned capacity [...]n if you do not

The DynamonDB free tier includes 100 MB of storage, 5 units of write capacity, and 10 units of read capacity per AWS account. This capacity is available to both existing and new AWS customers indefinitely.

Back Continue Help

© 2008 - 2013, Amazon Web Servic[...] Feedback

https console.aws.amazon.com/dynamodb/home?region=us-east-1#gs: — DynamoDB Management Console

Services Edit Marcel Dittkowski N. Virginia Help

Amazon DynamoDB Getting Started

Create Table Cancel

PRIMARY KEY | ADD INDEXES (optional) | PROVISIONED THROUGHPUT CAPACITY | THROUGHPUT ALARMS (optional) | SUMMARY

Throughput Alarms (optional)

☑ **Use Basic Alarms**

Notify me when my table's request rates exceed 75% of Provisioned Throughput for 60 minutes.

Notification will be sent when:

- Read Capacity Units consumed > 7.5

or

- Write Capacity Units consumed >3.75

Send notification to:

dhbw.nosql@gmail.com

Additional charges may apply if you exceed the AWS Free Tier levels for CloudWatch or Simple Notification Service.

Advanced alarm settings are available in the CloudWatch Management Console.

Back Continue Help

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Feedback

https console.aws.amazon.com/dynamodb/home?region=us-east-1#gs: — DynamoDB Management Console

Services Edit Marcel Dittkowski N. Virginia Help

Amazon DynamoDB Getting Started

Create Table Cancel

PRIMARY KEY | ADD INDEXES (optional) | PROVISIONED THROUGHPUT CAPACITY | THROUGHPUT ALARMS (optional) | SUMMARY

Review

Review the specifications for the table. Be aware that the hash key, range key, and local secondary index details cannot be changed after the table is created.

Primary Key Type: Hash and Range
Hash Key Attribute: user_id (String)
Range Key Attribute: name (String)
Provisioned Read Throughput: 10 units
Provisioned Write Throughput: 5 units
Estimated Provisioned Throughput Cost: $3.39 / month
Use Basic Alarms: Yes
Alarm Threshold: 75%
Alarm Notification Recipients:
Indexes:

Index Type	Index Hash Key	Index Range Key	Index Name	Projected Attributes
This table will not have any indexes.				

Back Creating Help

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Feedback

Anhang 23: AWS DynamoDB – Übersicht der vorhandenen Tabellen

Nach der Erstellung einer Datenbank gelangt der Kunde zur Übersicht seiner Tabellen. In diesem Menü erhält der Nutzer unter anderem Auskunft über den aktuellen Status und die Auslastung seiner Tabellen.

Amazon DynamoDB Tables

Name	Status	Hash Key	Range Key	Read Throughput	Write Throughput
DHBW-Test	CREATING	user_id	name	10	5

Table Items

Details | Indexes | Monitoring | Alarm Setup

CloudWatch Alarms: 2 of 2 in INSUFFICIENT DATA

Alarm History (past 24 hours): No alarms triggered

Time Range: Last Hour

Below are your CloudWatch metrics for the selected resources. Click on a graph to see an expanded view. View all CloudWatch metrics

Read Capacity (Units/Second - 5 Minute Average)

Throttled Read Requests (Count)

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Anhang 24: AWS DynamoDB – Anlegen von Datensätzen

Sobald die Tabelle den Status aktiv erreicht hat, können über die Menüleiste Datensätze erstellt werden (1). Der Kunde kann dabei beliebige Attribute mit den Datentypen Zahlen, Zeichenfolgen und Binärdaten anlegen.

Anhang 25: AWS DynamoDB – Schemalos

https console.aws.amazon.com/dynamodb/home?region=us-east-1#explore:name=DHBW-Test — DynamoDB Management Console

Services Edit Marcel Dittkowski N. Virginia Help

Amazon DynamoDB Explore Table: DHBW-Test

List Tables | Browse Items | Item Details

Scan Query Go New Item 1 to 3 of 3 loaded items

user_id	name	geheimdienst	musikgruppe	prename
"001"	"Jagger"			"Mick"
"007"	"Bond"	"MI6"		
"002"	"Lennon"		"Beatles"	

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Feedback

In der obigen Abbildung ist die Schemalosigkeit von NoSQL Datenbanken zu erkennen. Die unterschiedlichen Datensätze einer Tabelle können verschiedene Attribute besitzen, was in relationalen Datenbanken nicht möglich wäre.

Anhang 26: AWS Support – Preise im Überblick

AWS Support – Preise

Select an AWS Support Plan

Alle AWS Support-Stufen bieten eine unbegrenzte Anzahl von Support-Vorgängen ohne langfristige Verträge. Business- und Enterprise-Kunden erhalten außerdem bei zunehmenden AWS-Gebühren Volumenrabatte auf Ihre AWS Support-Kosten. Mithilfe des Rechners können Sie eine für Sie spezifische Schätzung der Bereitstellungskosten für AWS Support erstellen.

	Basic	Developer	Business	Enterprise
Preise	Enthalten	49 USD/Monat	Mehr als 100 USD – oder – 10 % der monatlichen AWS-Nutzung für die ersten 0 – 10 000 USD 7 % der monatlichen AWS-Nutzung für die ersten 10 000 – 80 000 USD 5 % der monatlichen AWS-Nutzung für die ersten 80 000 – 250 000 USD 3 % der monatlichen AWS-Nutzung ab 250 000 USD Preisbeispiel	Mehr als 15 000 USD – oder – 10 % der monatlichen AWS-Nutzung für die ersten 0 – 150 000 USD 7 % der monatlichen AWS-Nutzung von 150 000 – 500 000 USD 5 % der monatlichen AWS-Nutzung von 500 000 – 1 Mio. USD 3 % der monatlichen AWS-Nutzung ab 1 Mio. USD Preisbeispiel

Anhang 27: AWS Support – Funktionen im Überblick

AWS Support – Funktionen

AWS Support bietet Kunden, die technische Hilfe benötigen, einen individuell zugeschnittenen Service. Kunden, die sich nicht für AWS Support entscheiden, steht weiterhin unser Basic Support zur Verfügung, der ohne zusätzliche Kosten Zugriff auf das Ressourcenzentrum, häufig gestellte Fragen zu Produkten, Diskussionsforen und Support für Zustandsprüfungen bietet.

	Basic	Developer	Business	Enterprise
Kundendienst – Das ganze Jahr rund um die Uhr	✔	✔	✔	✔
Support-Foren	✔	✔	✔	✔
Dokumentation, Whitepaper, Anleitungen mit empfohlenen Vorgehensweisen	✔	✔	✔	✔
Zugang zu technischem Support	Unterstützung für Zustandsprüfungen (was ist das?)	E-Mail (landesspezifische Geschäftszeiten)	Telefon, Chat, E-Mail, Live-Bildschirmfreigabe (rund um die Uhr)	Telefon, Chat, E-Mail, Live-Bildschirmfreigabe, TAM (rund um die Uhr)
Bevorzugte Vorgangsbearbeitung	Technischer Kundenservicemitarbeiter	Cloud-Support-Mitarbeiter	Cloud-Support-Techniker	Leitender Cloud-Support-Techniker
Benannte Kontakte (was ist das?)		1	5	Unbegrenzt
Reaktionszeit		<12 Stunden	<1 Stunde	<15 Minuten
Architektur-Support (was ist das?)		Bausteine	Anleitung zu Anwendungsfällen	Anwendungsarchitektur
Anleitung mit empfohlenen Vorgehensweisen		✔	✔	✔
Kundenseitige Diagnosetools		✔	✔	✔
Identity Access Management (IAM) (Was ist das?)			✔	✔
Zugriff auf Support-API – Beta (was ist das?)			✔	✔
Support für die Software von Drittanbietern – Beta (was ist das?)			✔	✔
AWS Trusted Advisor – Beta (was ist das?)			✔	✔
Infrastructure Event Management (was ist das?)			Informationen zu Gebühren anfordern	✔
Direkter Kontakt zum Technical Account Manager (TAM)				✔
Weiterleitung von Vorgängen von Enterprise-Kunden (was ist das?)				✔
Geschäftsberichte für die Unternehmensleitung (was ist das?)				✔

7 Quellenverzeichnisse

Literaturverzeichnis

Baun, C./Kunze, M./Nimis, J./Tai, S. (2011): Cloud Computing – Web-basierte dynamische IT-Services, 2. Auflage, Heidelberg: Springer-Verlag

Edlich, S./Friedland, A./Hampe, J./Brauer, B. (2010): NoSQL – Einstieg in die Welt nicht-relationaler Web 2.0 Datenbanken

Metzger, C./Reitz, T./Villar, J. (2011): Cloud Computing – Chancen und Risiken aus techni scher und unternehmerischer Sicht, München: Carl Hanser Verlag

Terplan, K./Voigt, C. (2011): Cloud Computing, Heidelberg: mitp Verlag

Verzeichnis der Internet- und Intranet-Quellen

AWS (2013a): Amazon Web Services, http://aws.amazon.com/de/, Abruf: 09.01.2014

AWS (2013b): DynamoDB, http://aws.amazon.com/de/dynamodb/, Abruf: 10.01.2014

BDSG (2010): Bundesdatenschutzgesetz, http://www.bfdi.bund.de/cae/servlet/contentblob/409518/publicationFile/25234/BDSG.pdf Abruf: 12.01.2014

Bothe,S. (2012): Datenschutz und Datensicherheit im Cloud Computing, http://eddi.informatik.uni-bremen.de/SUSE/pdfs/Diplomarbeit_Steffen_Bothe.pdf, Ab ruf: 23.12.2013

Brown, C. (2011): NoSQL Tips and Tricks, http://blog.nosqltips.com/2011/04/cap-diagram-for-distribution.html, Abruf: 11.01.2014

BSI (2012): Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile, Abruf: 03.01.2014

Business-Cloud.de (2010): Alles Windows, oder was? Microsofts Cloud-Computing-Platt form Azure, http://www.business-cloud.de/alles-windows-oder-was-micorosofts-cloud-computing-plattform-azure/, Abruf: 15.01.2014

DB Engines (o. J.): Berechnungssmethode der Wertungen im DB-Engines Ranking, http://db-engines.com/de/ranking_definition, Abruf: 15.01.2014

Findling, T./König, T. (o. J.): MapReduce – Konzept, http://dbs.uni-leipzig.de/file/seminar_0910_findling_K%C3%B6nig.pdf, Abruf: 11.01.2014

Kuhn, F./Boutellier, R. (2012): Consensus Protekolle, http://web.fhnw.ch/plattformen/mvdbs/modulunterlagen/paxos, Abruf: 15.01.2014

MongoHQ (o. J.): MongoDB - Plans & Pricing with MongoHQ, https://www.mongohq.com/pricing, Abruf: 18.01.2014

Mongolab (2014): Database-as-a-Service by Mongolab, https://mongolab.com/, Abruf: 12.01.2014

o. V. (2010): NoSQL – Jenseit der relationalen Datenbanken, http://www.pro-linux.de/artikel/2/1455/3,einleitung.html, Abruf: 30.12.2013

o. V. (2011a): Spaltenorientierte Datenbanksysteme, http://wikis.gm.fh-koeln.de/wiki_db/Datenbanken/SpaltenorientierteDatenbank; Abruf: 30.12.2013

o. V. (2011b): MVCC - Multiversion Concurrency Control, http://wikis.gm.fh-koeln.de/wiki_db/Datenbanken/MVCC; Abruf: 30.12.2013

o. V. (2013a): Dokumentenorientierte Datenbank, http://wikis.gm.fh-koeln.de/wiki_db/Datenbanken/DokumentenorientierteDatenbank, Abruf: 30.12.2013

o. V. (2013b): Key/Value-Datenbanksysteme, http://wikis.gm.fh-koeln.de/wiki_db/Datenbanken/KeyValueSysteme, Abruf: 03.01.2014

o. V. (2013c): Graphendatenbank, http://wikis.gm.fh-koeln.de/wiki_db/Datenbanken/Graphendatenbank, Abruf: 03.01.2014

o. V. (2013d): MapReduce, http://de.wikipedia.org/wiki/MapReduce, Abruf: 10.01.2014

o. V. (2014a): NoSQL, http://de.wikipedia.org/wiki/NoSQL, Abruf: 20.01.2014

o. V. (o. J.): Graph database, http://en.wikipedia.org/wiki/Graph_database, Abruf: 03.01.2014

ObjectRocket (o. J.): ObjectRocket - Industrial Strength MongoDB http://www.objectrocket.com/pricing, Abruf: 18.01.2014

DHBW
Duale Hochschule
Baden-Württemberg
Stuttgart

AusweisApp Bund vs. BürgerApp Open eCard

Ein Vergleich der bestehenden Programme für die Online-Authentisierung in Verbindung mit dem neuen Personalausweis

Schriftliche Ausarbeitung
im Rahmen der Lehrveranstaltung „Integrationsseminar“

Vorgelegt von

Annika Kunde
Isabel Shen
Tobias Tröndle
Cathrin Kahre

am 31.01.2014

Fakultät Wirtschaft
Studiengang Wirtschaftsinformatik
WI-2011 I

Inhaltsverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface
APK	Android Application Package File
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien eV.
biw AG	Bank für Investments und Wertpapiere AG
BND	Bundesnachrichtendienst
bpb	Bundeszentrale für politische Bildung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAN	Customer Access Number
CIO	Chief Informational Officer
CORS	Cross-Origin Resource Sharing
DKB	Deutsche Kreditbank AG
EAC	Extended Access Control
eGK	Elektronische Gesundheitskarte
eID	Elektronische Identität
ELENA	Elektronische Einkommensnachweis
ELSTER	Elektronische Steuererklärung
ePA	Elektronischer Personalausweis
ePass	Elektronischer Reisepass
ESR	Extended Support Release
EU	Europäische Union
FAQ	Frequently Asked Questions
GDV	Gesamtverband der deutschen Versicherungswirtschaft
HPI	Hasso-Plattner-Institut
IT	Informationstechnologie
KfZ	Kraftfahrzeug
KKH	Kaufmännische Krankenkasse
MB	Megabyte
NSA	National Security Agency

PACE	Password Authenticated Connection Establishment
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung
SE	Standard Edition
SOP	Same-Origin-Policy
SSL	Secure Socket Layer
StGB	Steuergesetzbuch
SWOT	Strengths, Weaknesses, Opportunities, Threats
TAN	Transaktionsnummer
TKG	Telekommunikationsgesetz
USA	United States of America
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

Abbildungsverzeichnis

1 Einleitung

Der neue Personalausweis ermöglicht eine Authentifizierung im Internet, wodurch insbesondere die Kommunikation zwischen dem Bürger und Bürgerdiensten, Versicherungen und Finanzinstitutionen vereinfacht werden soll.[1] Darüber hinaus stehen den Bürgern weitere Services zur Verfügung, wie zum Beispiel die Anmeldung zum Lastschriftverfahren der Deutschen Bahn oder die Einrichtung und Anmeldung zu einem De-Mail-Konto, welche von der Telekom und der mentana claimsoftware angeboten werden.[2]

Am 8. November 2010 wurde diese Anwendungsform des neuen Personalausweises eingeführt.[3] Seither gerät die vom Bundesministerium finanzierte Software immer wieder unter Kritik, da ihr Quellcode nicht öffentlich zugänglich ist. Sicherheitsexperten äußern Bedenken, welche sich auf unentdeckte Sicherheitslücken und einer möglichen Gefahr der Datensicherheit durch voranschreitende staatliche Überwachung gründen. Außerdem ist die Anwendung nicht mit allen Versionen der üblichen Internet-Browser kompatibel, was die Bürger im Umgang mit dem neuen Personalausweis stark einschränkt.[4]

Das Projekt „Open eCard“ hat in Folge der Kritik an der AusweisApp die sogenannte BürgerApp entwickelt, welche ihren Quellcode offen legt. Somit ist hier der in Java programmierte Softwarecode für alle zugänglich und mögliche Sicherheitslücken können schneller identifiziert werden. Außerdem ist die Nachvollziehbarkeit der Datenspeicherung gewährleistet, womit die Hauptkritikpunkte an der AusweisApp gelöst werden können.

Das Unternehmen lässt im Folgenden prüfen, ob eine Verwendung der Online-Authentifizierungsfunktion für ihre Zwecke von Nutzen ist und welche der beiden Softwarelösungen ihren Anforderungen in größerem Maße gerecht wird. Im Unternehmen soll die AusweisApp oder die BürgerApp in einem „single-sign-on-Verfahren“ für ein Online-Portal zum Einsatz kommen. Die vom Unternehmen angeführten Vergleichsaspekte beider Lösungen sind die Sicherheit mit Bezug auf den Datenschutz und mögliche Risiken sowie die verwendeten Ressourcen, wozu der Festplattenspeicher und die PC-Anforderungen zählen. Weiterhin soll die Kompatibilität der Kartenlesegeräte, der Internet-Browser und des Betriebssystems geprüft werden. Schließlich soll auch der benutzerfreundliche Umgang für den Kunden und die Administration einschließlich bereitstehender Supportfunktionen für Unternehmen untersucht werden. Im Ergebnis wird basierend auf dem Vergleich beider Softwarelösungen eine Empfehlung gegeben und mögliche Alternativen aufgezeigt.

---

[1] Vgl. Bundesministerium des Innern (2013a)
[2] Vgl. Bundesministerium des Innern (2013b)
[3] Vgl. Bundesministerium des Innern (2013c)
[4] Vgl. AusweisApp-Portal (o.J. a)

1.1 Aktualität des Themas

Artikel 10 der Grundrechte des Menschen besagt:

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

Dieser Grundsatz untersagt es, dass Fernmeldebotschaften abgehört, unterdrückt oder entstellt werden. Zu Fernmeldebotschaften zählen Schreib-, Fernsprech- und Funknachrichten. Der § 88 des Telekommunikationsgesetzt (TKG) besagt:

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

Dieses Gesetz dient dem Schutz der Privatsphäre jedes einzelnen und der Informationen, die an individuelle Empfänger gerichtet sind.

In § 39 des Postgesetzes heißt es:

(1) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter natürlicher oder juristischer Personen sowie der Inhalt von Postsendungen.

Dieses Gesetz ist vom Briefgeheimnis abzugrenzen, welches alle schriftlichen Mitteilungen zwischen Absender und individuellem Empfänger schützt, während das Postgeheimnis alle von der Post übermittelten Sendungen sichert.

Geahndet werden Verstöße gegen diese Gesetze im § 206 des Steuergesetzbuchs (StGB):

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigten eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Im Zusammenhang mit diesen Gesetzen steht eine Thematik, die Mitte 2013 von den Medien große Beachtung geschenkt bekommt und viele Bürger über den Verbleib ihrer Daten aus Telefongesprächen, E-Mails und anderer Nachrichtendienste verunsichert. Das Thema Datensicherheit hat vor dem Hintergrund des US-Geheimdienstes NSA (National Security Agency) seit Anfang Juni 2013 an Brisanz zugenommen. Zu diesem Zeitpunkt heißt es, die NSA soll Zugriff auf Telekommunikationsdaten des US-Telekomkonzerns Verizon haben. Hierbei werden Rufnummern, Uhrzeit und Dauer von Telefonaten verfolgt und gespeichert. Die Regierung rechtfertigte sich, dass diese Aktivitäten terroristischen Angriffen vorbeugen

würden. Die Quelle dieser Anschuldigungen ist der Ex-NSA-Mitarbeiter Edward Snowden. Nur einen Tag später wird bekannt, dass die NSA direkten Zugriff auf die Server von neun Internetfirmen habe. Das hierfür verwendete Programm unter dem Namen „Prism" zeichnet unter anderem Fotos, Videos, E-Mails und Dokumente auf, um die „Kontakte und Bewegungen einer Person nachzuvollziehen"[5]. Die beschuldigten Internetfirmen beteuern, ohne entsprechende Gerichtsbeschlüsse keine Daten herausgegeben zu haben. Außerdem hätten sie noch nie von „Prism" gehört. In Folge dessen tritt der US-Geheimdienstkoordinator James Clapper an die Öffentlichkeit und gibt zu, dass „Prism" ausschließlich Daten von Nicht-Amerikanern außerhalb der USA sammle.

Die deutsche Bundesregierung bestreitet, etwas von den Aktivitäten der NSA gewusst zu haben. Bundesinnenminister Hans-Peter Friedrich verteidigt den US-Geheimdienst, da durch ihn und seine Informationen auch in Deutschland in der Vergangenheit Anschläge verhindert werden konnten. Auch US-Präsident Obama äußert sich bei einem Besuch in Berlin zur NSA-Affäre und räumt ein, dass „Prism" zur Verhinderung von mehr als 50 Anschlägen beigetragen habe und absolut legal sei.

In den folgenden Tagen werden Hinweise bekannt, die die systematische Ausspähung von Institutionen der Europäischen Union (EU) belegen. Der „Spiegel" veröffentlicht am 30. Juni 2013 Informationen, denen zu Folge im Deutschland mehr Daten von der NSA erfasst werden, als in jedem anderen Land. Die Spionage soll auch die Bundesregierung und Bundeskanzlerin Merkel betreffen, woraufhin die Regierung eine umfassende Aufklärung des Skandals fordert. Bis heute liegt jedoch kein öffentlicher Bericht der USA vor.

Seit Juli 2013 werden immer neue Details der NSA-Affäre bekannt. So bleibt unklar, in welchem Ausmaß der Bundesnachrichtendienst (BND) mit der NSA kooperierte. Außerdem berichten die „New York Times" und der „Guardian", dass die NSA verschlüsselte Kommunikation verfolgt und zudem auch E-Mails von US-Bürgern gespeichert werden.[6]

Die Bürger der Bundesregierung sind unterdessen verunsichert. Welche ihrer Daten werden gespeichert? Wie verhielte sich dies mit den sensiblen Daten des Personalausweises, die über einen Online-Server auf die entsprechenden Internetseiten von Bürgerdiensten, Versicherungen und Finanzinstitutionen übertragen werden?

Auf die Bedeutung der Datensicherheit für das Unternehmen soll im Folgenden Bezug genommen werden.

---

[5] Köhr, O. (2013)
[6] Vgl. ebenda

1.2 Datensicherheit als ausschlaggebender Faktor

Die Datensicherheit ist einer der zentralen Punkte dieser Studie. Obwohl das Thema Datenschutz und –sicherheit verstärkt erst seit den bereits erwähnten Enthüllungen durch Edward Snowden in den Fokus der Öffentlichkeit gelangt ist, beschäftigen sich Versicherungen schon viel länger damit.

Hauptgrund hierfür ist die ihnen gesetzlich auferlegte Verpflichtung zum besonders sorgfältigen Umgang mit persönlichen Daten Dritter:

„Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als [...] Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebens-versicherung [...] anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“

StGb, § 203 Abs. 1 Nr. 6

Der Gesetzgeber regelt diese Thematik ganz bewusst im Strafgesetzbuch, da es sich bei den Daten zum gesundheitlichen Zustand um höchst schützenswerte, persönliche Daten handelt, deren Weitergabe für den Betroffenen weitaus größere Folgen haben kann, als beispielsweise lediglich die Weitergabe des Geburtsdatums.

Versicherungen sind aber nicht nur aufgrund der gesetzlichen Regelungen am Schutz der Daten ihrer Kunden interessiert, sondern auch um das bestehende Vertrauensverhältnis zu schützen und aufrecht zu erhalten, in dessen Rahmen der Kunde seine persönlichen Daten an den Versicherer übergibt.

Seit der Entwicklung des PCs und der Möglichkeit, Daten elektronisch zu speichern, hat sich die gesamte Thematik Datensicherheit jedoch massiv verschärft und der Schutz von Daten ist um einiges schwieriger und komplexer geworden. Verdeutlichen lässt sich dies durch eine gängige Definition von Datensicherheit:

„Datensicherheit ist der angestrebte Zustand, der durch alle diese Maßnahmen erreicht werden soll, aber letztlich nicht vollkommen erreicht werden kann.“ [7]

Hierbei zeigt sich bereits, dass eine vollkommene Datensicherheit reine Utopie ist. Begründen lässt sich dies auch durch die Vielzahl an Einflussfaktoren, die in Hinblick auf Datenschutz beachtet werden müssen.

---

[7] Pommerening, K. (1991), S. 10

Erfolgt eine elektronische Speicherung von zu schützenden Daten, so ist neben dem physischen Schutz der Daten im Gebäude durch Zugangskontrollen, etc. eine Reihe weiterer virtueller Aspekte zu beachten. So müssen beispielsweise auch die Rechner über Zugangssperren verfügen, Firewalls müssen die Daten gegen Angriffe aus dem Internet schützen und idealerweise sollten die Daten durch Verschlüsselungstechniken zusätzlich gesichert sein.

Werden die Daten zudem auch noch über das Internet transferiert, lässt sich die Datensicherheit keinesfalls mehr garantieren, was in einem starken Kontrast zum Fernmeldegeheimnis steht, welches in der Bundesrepublik zu den Grundrechten zählt und daher wie bereits aufgezeigt im Artikel 10 des Grundgesetzes verankert ist.[8]

Unternehmen, die wie Versicherungen mit sensiblen Daten in Kontakt kommen, stehen nun vor einem Zwiespalt. Auf der einen Seite sind sie gesetzlich verpflichtet, die Daten ihrer Kunden zu schützen, was am besten funktionieren würde, wenn diese nicht über das Internet zugänglich gemacht würden, auf der anderen Seite verlangen die Kunden aber eben diesen Zugriff auf ihre persönlichen Angaben und wählen unter anderem nach diesem Kriterium aus, welchen Wettbewerber sie bevorzugen.

Da Versicherungen im Kampf gegen die Konkurrenz das Thema der Online-Bereitstellung von Daten für ihre Kunden also nicht vernachlässigen können, müssen die bestmöglichen technischen Schutzmaßnahmen implementiert werden, um sowohl den Kunden als auch dem Gesetzgeber zu verdeutlichen, dass alle Möglichkeiten zum Schutz der Daten ausgeschöpft wurden.

1.3 Vorgehensweise

Wie bereits in der Problemstellung beschrieben, interessiert sich das Unternehmen für eine Empfehlung für eines der beiden am Markt gängigen Programme zur Abwicklung der Identitätsprüfung mithilfe des neuen Personalausweises.

Zunächst wird hierzu der neue Personalausweis genauer vorgestellt und die Funktionalität der elektronischen Ausweis-Funktion erklärt. Zusätzlich sollen bereits existierende Einsatzbereiche vorgestellt werden. Eine Analyse über die Akzeptanz des neuen Personalausweises und insbesondere der elektronischen Ausweis-Funktion soll zudem die Möglichkeit bieten, eine erste Einschätzung über die Dringlichkeit, mit der das Thema weiterbearbeitet werden sollte, zu treffen.

[8] Vgl. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (o.J.)

Anschließend erfolgt eine detaillierte Analyse der beiden Programme. Diese werden zunächst in einer allgemeinen Einführung beschrieben und danach in Hinblick auf verschiedene Kriterien untersucht. Begonnen wird mit den Ressourcenanforderungen, gefolgt von Kompatibilität und dem wohl wichtigsten Kriterium, der Sicherheit.

Dazuhin sollen auch Benutzerfreundlichkeit sowie Administrations- und Supportmöglichkeiten untersucht werden, um einen umfassenden Eindruck über die beiden Programme zu erhalten. Zuletzt soll anhand einer SWOT-Analyse ein Überblick über Vor- und Nachteile des jeweils untersuchten Programms geschaffen werden.

Als Instrument zur strategischen Planung erscheint die SWOT-Analyse hier besonders geeignet. Die um 1960 an der Harvard Business School entwickelte Analyse beleuchtet systematisch die internen Stärken (Strengths) und Schwächen (Weaknesses) eines Unternehmens, eines Produktes oder einer Dienstleistung und schenkt gleichzeitig externen Faktoren in Form von Möglichkeiten (Opportunities) und Bedrohungen (Threats) Beachtung.[9]

Auf die Einzelanalyse der beiden Programme folgt ein Vergleich, der nun die zuvor festgestellten Vor- und Nachteile gegenüberstellend betrachtet und bewertet. Basierend auf diesem Vergleich, soll anschließend die Empfehlung für eines der beiden Programme erfolgen. Das Ergebnis beansprucht dabei keine generalisierende oder absolute Gültigkeit, sondern soll den speziellen Anforderungen des Unternehmens gerecht werden.

Abschließend sollen neben den beiden geprüften Programmen Alternativlösungen vorgestellt werden, welche ebenfalls die im Unternehmen definierten Anforderungen abdecken.

Im darauffolgenden Schlusswort werden die zuvor erarbeiteten Ergebnisse nochmals zusammenfassend rekapituliert.

[9] Vgl. Pelz, W. (2004)

2 Der neue Personalausweis

Als Folge des im Dezember 2008 verabschiedeten „Gesetzes über Personalausweise und den elektronischen Identitätsnachweis“, wurde am 01. November 2010 der neue Personalausweis eingeführt[10]. Das bisherige Ausweisdokument bleibt weiterhin gültig, bei Erstbeantragungen beziehungsweise Verlängerungen wird nun allerdings der neue Ausweis ausgestellt, der sowohl äußerlich als auch funktional überarbeitet wurde. Wie gewohnt, dient das Dokument als Sichtausweis; dank seiner neuen Funktionalitäten wird der Ausweis zukünftig aber auch die Online-Kommunikation zwischen Bürgern und Unternehmen oder auch Behörden vereinfachen und auf diese Art und Weise neue Einsatzbereiche finden[11].

Das folgende Kapitel dient der Vorstellung des neuen Personalausweises und wird daher zunächst seine Funktionalitäten und Einsatzbereiche erläutern. Den Abschluss bildet eine Beleuchtung der Akzeptanz des neuen Personalausweises in der Bevölkerung.

2.1 Funktionalitäten

Im Allgemeinen dient der Personalausweis als hoheitliches Dokument der Identifikation des Besitzers als Bürger der Bundesrepublik Deutschland[12]. Zu diesem Zweck gibt er Auskunft über bestimme Daten die in §5 des Personalausweisgesetzes einheitlich festgelegt sind[13]. Dazu zählen neben Angaben zur ausstellenden Behörde sowie der Gültigkeit des Dokuments unter anderem auch folgende Informationen über den Ausweisinhaber:[14] Familien-, Geburts- und Vornamen, Tag und Ort der Geburt, Größe, Augenfarbe, Anschrift, Staatsangehörigkeit, biometrisches Lichtbild sowie Unterschrift.

Der seit dem 1. November 2010 erhältliche, neue Personalausweis hebt sich sowohl äußerlich durch sein Scheckkartenformat als auch funktional von dem bisherigen Dokument ab[15]. Für die Einführung des überarbeiteten Ausweises, wurden die bestehenden Sicherheitsmerkale wie beispielsweise das komplexe holografische Reproduktionsmerkmal in Form des Identigrams® für das neue Format und Material nicht nur angepasst sondern auch verbessert[16]. Laut Aussage des Bundeskriminalamtes machen diese Funktionen den Personalausweis zu einem „hochsichere[n] Ausweisdokument, bei dem die bewährte Fälschungssicher-

---

[10] Vgl. Bundesministerium für Sicherheit in der Informationstechnik (o. J. a)
[11] Vgl. ebenda
[12] Vgl. Bundesministerium des Innern (2013d)
[13] Vgl. Bundesministerium der Justiz (o. J.)
[14] Vgl. ebenda
[15] Vgl. Bundesministerium des Innern (2010), S. 4
[16] Vgl. Bundesdruckerei GmbH (2010)

heit des bisherigen Ausweises konsequent für das Scheckkartenformat weiterentwickelt wurde"[17].

Neben diesen Änderungen stellt aber vor allem die Möglichkeit der online Nutzung durch die „Biometriefunktion, die Online-Ausweisfunktion und die elektronische Unterschriftsfunktion"[18] des Ausweises die wichtigste Neuerung dar. Die zuletzt genannte Funktion der „Qualifizierten Elektronischen Signatur" ermöglicht in Verbindung mit Signaturzertifikaten das rechtskräftige Unterzeichnen digitaler Dokumente[19].

Für den Zweck des Identitätsnachweises im Internet ist ein Sicherheits-Chip im Ausweis integriert, auf dem die persönlichen Daten inklusive Lichtbild sowie optional auch die Fingerabdrücke des Ausweisinhabers gespeichert sind[20]. Bild und Fingerabdrücke dienen dabei der hoheitlichen Identifikation und dürfen daher lediglich von bestimmten staatlichen Stellen wie Polizei und Grenzbehörde ausgelesen werden[21]. Auf diese Art und Weise wird die „Gefahr von Identitätsmissbrauch"[22] gesenkt, da die gespeicherten biometrischen Daten die Bindung zwischen Dokument und Besitzer stärken. Die übrigen personenbezogenen Daten können für die Online-Ausweisfunktion genutzt werden, die es dem Bürger erlaubt, seine „Identität bei elektronischen Anwendungen im Internet einfach, sicher und zuverlässig [zu] belegen"[23]. Diese Möglichkeit wird als „Ausweisfunktion, ‚Elektronischer Identitätsnachweis' (abgekürzt eID-Funktion), oder Authentisierungsfunktion bezeichnet und bildet das Kernstück des neuen Personalausweises"[24]. Anwendung findet dieses Prinzip beispielsweise bei „Online-Services von privatwirtschaftlichen Unternehmen wie Online-Shops oder Versicherungen"[25], um das Ausfüllen von Formularen zu automatisieren, sodass die manuelle Eingabe der persönlichen Daten entfällt. Gleichzeitig sollen die digitalen Daten zukünftig auch dem Ausweisen an Automaten, bei der Anmietung von Autos oder beim Hotel Check-in dienen und Behördengänge ersetzen. Behörden und Unternehmen müssen als Dienstanbieter dabei über ein Berechtigungszertifikat verfügen, das ihnen das Auslesen der gespeicherten Daten erlaubt. So wird gewährleistet, dass sich beide Seiten der Identität ihres Gegenübers sicher sein können[26].

---

[17] Seidel, U. (2011)
[18] Vgl. Bundesdruckerei GmbH (2010)
[19] Vgl. Bundesministerium des Innern (2013d)
[20] Vgl. Bundesministerium des Innern (2013c)
[21] Vgl. Bundesministerium des Innern (2013e)
[22] Bundesdruckerei GmbH (2013a)
[23] Bundesdruckerei GmbH (2010)
[24] Bundesamt für Sicherheit in der Informationstechnik (o. J. a)
[25] Bundesdruckerei GmbH (2013a)
[26] Vgl. Bundesdruckerei GmbH (2013b)

Die Nutzung der Ausweisfunktion für die internetbasierte beziehungsweise maschinelle Kommunikation geschieht dabei auf freiwilliger Basis, der Dokumenteninhaber kann die Funktion jederzeit bei der zuständigen Amtsstelle aktivieren beziehungsweise deaktivieren lassen[27]. Neben des Einschaltens der Funktion müssen noch weitere Voraussetzungen erfüllt sein, um die Authentisierungsfunktion nutzen zu können:[28] Bei Beantragung des neuen Personalausweises wird dem Besitzer ein Brief mit einer fünfstelligen Transport-Kennzahl übermittelt, die dieser in eine persönliche sechststelligen persönliche Identifikationsnummer (PIN) umwandeln muss. Bei Verwenden der Ausweisfunktion dient diese Nummer der Bestätigung zur verschlüsselten Datenübermittlung. Außerdem muss der Dokumenteninhaber zusätzlich über ein personalausweisfähiges Kartenlesegerät sowie eine entsprechende Software verfügen, die die Verbindung zwischen dem Personalausweis und dem PC herstellt und die verschlüsselte Datenübertragung ermöglicht.

Das Online-Ausweisen funktioniert schließlich folgendermaßen:[29] Der Nutzer entschließt sich für den Kauf eines Produktes in einem Online-Shop, der für die Rechnungszustellung und den Versand die personenbezogen Angaben wie Name und Anschrift benötigt. Dank des neuen Personalausweises können diese Informationen bequem an das Unternehmen übermittelt werden. Alle Internetseiten, die die Online-Ausweisfunktion unterstützen sind dabei durch folgendes Logo gekennzeichnet:

Der neue
Personalausweis

Abb. 1: Logo des neuen Personalausweises[30]

Zur tatsächlichen Informationsübertragung wird zunächst das Berechtigungszertifikat des Händlers angezeigt, das Angaben zum Anbieter selbst sowie zur Gültigkeit des Zertifikats enthält. An dieser Stelle kann der Benutzer explizit auswählen, welche Daten er dem Anbieter übermitteln möchte. Nach Bestätigung des Vorgangs durch Eingabe der sechsstellige PIN, wird automatisch im Chip des Ausweisdokumentes einerseits das Berechtigungszertifikat des Händlers und andererseits die Gültigkeit des Personalausweises überprüft. Erst dann werden die freigegebenen Daten verschlüsselt an den Online-Shop übertragen. Aus Sicherheitsgründen erfolgt die beidseitige Prüfung dabei nicht durch den Anbieter des Dienstes, sondern über einen sogenannten eID-Server, um auszuschließen, dass der Händler direkt

[27] Vgl. Bundesdruckerei GmbH (2013a)
[28] Vgl. Bundesamt für Sicherheit in der Informationstechnik (o. J. b)
[29] Vgl. Bundesministerium des Innern (2010), S. 12
[30] Enthalten in: Bundesministerium für Sicherheit in der Informationstechnik (o.J. b)

auf die Daten zugreifen kann[31]. Kapitel 2.4 wird dabei den eID Server näher beleuchten; eine detaillierte Illustration des achtstufigen Vorgangs beim Online-Ausweisen kann in *Anhang 1* gefunden werden.

Insgesamt steht die Datensicherheit beim neuen Personalausweis im Vordergrund. Sowohl die Verschlüsselung der Datenübertragung als auch die Tatsache, dass ein Auslesen aus der Ferne nicht möglich ist, da immer der Ausweis in Kombination mit der PIN benötigt wird, schützen die persönlichen Daten vor Missbrauch im Internet. Zusätzlich gilt das Prinzip der Datensparsamkeit, das sicherstellt, dass lediglich die nötigen Informationen übertragen werden – für bestimmte Dienste gegebenenfalls auch nur eine Altersbestätigung in Form von „ja" oder „nein" statt des Geburtsdatums[32].

Alles in allem sind die Funktionen des neuen Personalausweises darauf ausgerichtet, dass ein gesteigertes „Maß an gegenseitigem Vertrauen"[33] geschaffen werden kann, um auch im Internet eine sichere Authentifizierung zu ermöglichen. Unternehmen können sich so einen Wettbewerbsvorteil schaffen, da sie die Kommunikation mit dem Kunden leichter und bequemer gestalten und die Zufriedenheit durch reduzierte Wartezeiten steigern[34]. Diese Möglichkeiten entsprechen den aktuellen Entwicklungen des täglichen Lebens, das sich zunehmend in die online Welt verlagert.

2.2 Einsatzbereiche

Viele Aktivitäten und Geschäfte des Alltags finden mittlerweile im Internet statt. Mit der neuen Online-Ausweisfunktion können Bürgerinnen und Bürger ihre Identität im Internet sicher und eindeutig belegen, sowie auch die des Gegenübers im Netz zuverlässig feststellen.

Wie im vorhergegangenen Abschnitt erläutert, sind auf dem Chip des neuen Personalausweises Daten, wie z.B. Vor- und Familienname, Geburtstag, Geburtstort und Anschrift gespeichert.[35] Die Online-Funktion kann somit z.B. die Alters- oder Wohnortsbestätigung im Internet erleichtern: Manche Dienstleistungen dürfen nur von Nutzern in Anspruch genommen werden, die ein bestimmtes Alter erreicht haben oder an einem bestimmten Wohnort

[31] Vgl. Bundesministerium des Innern (2013f)
[32] Vgl. Bundesministerium des Innern (2013g)
[33] Bundesdruckerei GmbH (2013c)
[34] Vgl. ebenda
[35] Vgl. Bundesministerium des Innern (2012)

gemeldet sind. Der neue Personalausweis kann Alter oder Wohnort bestätigen, ohne weitere, genaue Daten zu übermitteln.[36]

Die Online-Ausweisfunktion wird vor allem von Diensten angeboten, die ihre Registrierungsvorgänge für den Nutzer einfacher und sicherer gestalten möchten.[37] Viele Branchen profitieren bereits jetzt von der neuen Online-Ausweisung. Einsatzbeispiele finden sich in Bereichen der Behördendienste, Versicherungen, Finanzen etc., die im Folgenden näher aufgezeigt werden.

Das breiteste Angebot mit der neuen Online-Ausweisfunktion stellen öffentliche Behörden zur Verfügung, mit denen Bürgerinnen und Bürger Zeit und Aufwand sparen können.

- In vielen Bundesländern, wie z.B. Baden-Württemberg und Bayern, ermöglicht die Online-Ausweisfunktion des neuen Personalausweises, sich über ein Portal sicher zu registrieren und anzumelden, um Behördengänge im Internet zu erledigen. Durch die Eingabe der PIN autorisiert der Benutzer den Behörden, Daten wie Name, Geburtsdatum und Anschrift, vom Kartenlesegerät auszulesen und mittels einer Verbindungs-Software geschützt zu übertragen. So bieten viele Länder- und Kommunen-Portale an, persönliche und sensible Daten und Dateien, wie z.B. die Geburtsurkunde, in einem Datenspeicher verschlüsselt abzulagern – eine Art „Dokumentensafe“.[38] Nutzerinnen und Nutzer haben orts- und zeitunabhängige die Möglichkeit, diese Dokumente elektronisch an Behörden weiterzuleiten.[39] Dies erspart den Benutzern einerseits den Gang zum Amt und entlastet gleichzeitig die Behörden. Weitere Dienste, die bereits viele Länder anbieten, sind unter anderem Dienstleistungen für Kraftfahrzeuge (KfZ), wie z.B. die Zulassung von Neuwagen, die elektronische Einreichung der Steuererklärung oder die Beantragung von Bescheinigungen und Urkunden. Mit der Online-Ausweisfunktion können Bewohner der Stadt Bielefeld im Online-Portal sogar Wahlscheine und Stimmzettel für Wahlen und Bürgerentscheide beantragen.[40]

- Die Bundesbehörde Bundesagentur für Arbeit bietet auf ihrer Webseite Anwendungen an, mit denen Nutzerinnen und Nutzer sich über ihren Antragstatus für deren Kindergeldbezug informieren oder persönlichen Daten online ändern können.[41] Die deutsche Rentenversicherung erlaubt die Online-Abfrage des eigenen Rentenkontos, des historischen Versicherungsverlaufs und der individuellen Beitragsberechnung.

[36] Vgl. Bundesministerium des Innern (2012)
[37] Vgl. Bundesministerium des Innern (2013h)
[38] Vgl. Bundesministerium des Innern (2013i)
[39] Vgl. ebenda
[40] Vgl. ebenda
[41] Vgl. Bundesministerium des Innern (2013i)

Sensible Daten, wie Daten bezüglich der Bankverbindung lassen sich ebenfalls mit der elektronischen Ausweisung online ändern.[42]

Finanzdienstleistungen wie die oben erwähnte elektronische Abgabe der Steuererklärung laufen über das Online-Portal für die elektronische Steuererklärung (ELSTER). Dieses wurde 2009 zur sicheren Online-Kommunikation mit dem deutschen Finanzamt mithilfe der elektronischen Ausweisung errichtet.[43] Als eine Art „elektronisches Finanzamt“ können dank ElsterOnline Steuerbelange am Computer ohne Ausdrucke, Formulare und Postversand erledigt werden.[44] Die Anmeldung und Authentifizierung funktioniert mit dem neuen Personalausweis. Der Service kann nach der Registrierung von Steuerbürgern, Steuerberatern, Lohnsteuerhilfevereinen und Stellvertretern von Unternehmen genutzt werden.[45]

- ElsterOnline bietet eine Reihe von Formularen, die online ausgefüllt und abgegeben werden können, z.B. die Einkommensteuererklärung, die Lohnsteuerbescheinigung oder die Umsatzsteuer-Voranmeldungen.[46]
- Neben der Bereitstellung von Formularen können auch Dienste, wie z.B. die Auskunft zur elektronischen Lohnsteuerkarte oder die Steuerkontoabfrage durch das ElsterOnline-Portal in Anspruch genommen werden.[47]

Praktisch ist, dass der neue Personalausweis eine Wiedererkennungsfunktion, das sogenannte Single Sign-on Verfahren, besitzt: Online-Dienste können registrierte Nutzer nach einer einmaligen Autorisierung mit der sogenannten Pseudofunktion wiedererkennen.[48] Bei ElsterOnline kann ein Nutzerprofil mit Daten angelegt werden, die über die Anmeldezeiträume hinweg gleich bleiben, wie z. B. Name, Steuernummer, Telefonnummer etc. Beim Ausfüllen eines Formulars kann ein entsprechendes Profil ausgewählt werden und die zugehörigen Profildaten werden automatisch in das Formular eingefüllt, so dass das Ausfüllen von Formularen deutlich beschleunigt wird.

Auch Versicherungsunternehmen können einen großen Nutzen aus der Online-Funktion des neuen Personalausweises ziehen. Führende Versicherungen wie die Allianz, die Techniker Krankenkasse oder CosmosDirekt bieten auf ihren Online-Kundenportalen bereits jetzt eine Vielzahl von Diensten an, die mit der die Online-Ausweisfunktion von den Nutzerinnen und Nutzern in Anspruch genommen werden können.

---

[42] Vgl. ebenda
[43] Vgl. ubuntuusers.de (2013)
[44] Vgl. Bundesministerium des Innern (2013j)
[45] Vgl. ELSTER (2013a)
[46] Vgl. ELSTER (2013b)
[47] Vgl. ebenda
[48] Bundesministerium des Innern (2012)

– Zum Beispiel können sich Kunden im Online-Kundenportal der jeweiligen Versicherung mit der neuen Ausweisfunktion nach der Registrierung einfach und sicher anmelden. Auf dem Portal können dann sensible Versicherungsdaten eingesehen werden. Bei manchen Versicherungen, wie bei HUK24, ist es bereits möglich, die Versicherung komplett online zu verwalten – egal, ob ein Vertrag abgeändert oder eine neue Versicherung abgeschlossen werden soll.[49]
– Außerdem besteht bei mehreren Versicherungsunternehmen die Möglichkeit, Unterlagen, wie z.B. Versicherungsbescheinigungen oder neue Versicherungskarten, online anzufordern oder persönlichen Daten, z. B. Adresse und Bankverbindung, mit wenigen Klicks zu ändern.[50]
– Versicherungen können zudem individuell auf den Kunden zugeschnittene Angebote machen. So bietet die Kaufmännische Krankenkasse (KKH) Nutzerinnen und Nutzern ihres Online-Services an, Medikamente zu Sonderkonditionen zu bestellen und exklusive Angebote zu nutzen.[51]

Der Gesamtverband der deutschen Versicherungswirtschaft (GDV) fördert mithilfe des neuen Personalausweises die elektronische Kommunikation zwischen Versicherungsunternehmen und unabhängigen Versicherungsvermittlern, indem es ein Single Sign-On-Portal zur Verfügung stellt, das den Vermittlern „einen zentralen Zugriff auf die Maklerportale der einzelnen Versicherungsunternehmen ermöglicht“.[52] Vermittler müssen sich somit nicht jedes Mal an den diversen Unternehmensportalen über unterschiedliche Verfahren autorisieren, sondern können sich künftig über die Anmeldung am GDV-Marklerportal auf die verschiedenen Unternehmensportale nach einer einmaligen Autorisierung beim Unternehmensportal zugreifen.[53]

Auch Bankunternehmen können mit dem neuen Personalausweises neue Services auf ihren Webseiten anbieten, wie beispielsweise die Online-Eröffnung eines Bankkontos. Mithilfe der Online-Ausweisfunktion werden die durch eine PIN autorisierten Daten vom Kartenlesegerät ausgelesen und via Verbindungssoftware geschützt übertragen. Anschließend vervollständigen Kunden den Antrag um zusätzliche Informationen und können damit die Kontoeröffnung abschließen.[54] Die Online-Ausweisfunktion dient dabei als schnelle und sichere Alternative

[49] Vgl. Bundesministerium des Innern (2013k)
[50] Vgl. ebenda
[51] Vgl. ebenda
[52] GDV Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2013)
[53] Vgl. ebenda
[54] Vgl. Bundesministerium des Innern (2013l)

zum PostIdent-Verfahren und garantiert eine sofortige Abwicklung der Registrierung. Diese Funktion bietet z.B. die Deutsche Kreditbank AG (DKB) an.[55]

Ein weiteres Einsatzbeispiel im Bereich der Finanzen bietet die Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) an: Nutzerinnen und Nutzer können sich einfach und sicher im Kundenportal der Schufa mit dem neuen Personalausweis registrieren und online ausweisen. Ohne weitere Verzögerungen haben diese nach Anmeldung im Portal die Möglichkeit, ihre Schufa-Auskunft direkt online abzurufen oder auf dem Postweg ihren Geschäftspartnern zukommen zu lassen.[56]

Wie erwähnt, können Bürgerinnen und Bürger mit der Online-Ausweisfunktion des neuen Personalausweises ihre Identität nicht nur im Internet eindeutig belegen, sondern auch an Automaten und Selbstbedienungsterminals. So bietet die Bank für Investments und Wertpapiere AG (biw AG) für Kundinnen und Kunden deutscher Kreditinstitute die Möglichkeit, gebührenfrei Bargeld mit dem neuen Personalausweis abzuheben.[57] Dazu müssen diese sich am Geldautomaten mit dem neuen Personalausweis und ihrer PIN einmalig für das Lastschriftverfahren anmelden. Den ausgezahlten Betrag bucht die biw AG dann gebührenfrei vom hinterlegten Konto ab. Der erste Geldautomat, an dem dieser Service genutzt werden kann, steht in der Bundesdruckerei in Berlin; weitere Standorte sind in Planung.[58]

Es gibt viele weitere Einsatzbereiche des neuen Personalausweises, die von Unternehmen wie die Deutsche Bahn, Telekom, diversen Hochschulen etc. bereits heute wahrgenommen und angeboten werden.[59] Die Möglichkeiten zum Einsatz der Online-Ausweisfunktion sind noch nicht ausgeschöpft und es ist zu erwarten, dass das Angebot in den kommenden Jahren deutlich zunehmen wird.

2.3 Akzeptanz in der Bevölkerung

Im Folgenden soll darauf eingegangen werden, welche Akzeptanz der überarbeitete Personalausweis mit seinen neuen Funktionalitäten in der Bevölkerung findet.

Schon vor dem 1. November 2010 hat die ARIS Umfrageforschung Markt-, Media- und Sozialforschungsgesellschaft mbH im Auftrag des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) eine telefonische Umfrage unter 1.004

[55] Vgl. ebenda
[56] Vgl. Bundesministerium des Innern (2013l)
[57] Vgl. ebenda
[58] Vgl. ebenda
[59] Vgl. Bundesministerium des Innern (2013m)

Deutschen durchgeführt, um sich ein Meinungsbild über den bevorstehenden Wechsel zum neuen Personalausweis zu verschaffen. Neben Alter und Geschlecht wurde auch die Internetnutzung als Unterscheidungskriterium hinzugezogen. Die Ergebnisse können dabei folgendermaßen zusammengefasst werden:[60]

- Das Internet wird von rund 70% der Deutschen genutzt, wobei der Anteil bei dem Bevölkerungsanteil zwischen 14 und 29 Jahren bei fast 100% liegt, bei den Älteren über 65 Jahren nur noch 32%.
- Der Einführung des neuen Personalausweises sahen die Deutschen mit sehr gemischten Gefühlen entgegen: Während 46 % den Wechsel begrüßten, sahen 45 % dem eher kritisch entgegen. Hier muss auch festgehalten werden, dass die Internetnutzer zu immerhin 52% das neue Dokument begrüßen, während der Anteil bei den Nicht-Internet-Nutzern bei lediglich 32% lag.
- Vor allem Behördengänge könnten durch den neuen Personalausweis vereinfacht werden, da fast jeder zweite Internetnutzer (44%) die Ausweisfunktion für E-Government-Dienste wie Um- und Anmeldungen nutzen würde. Weitere Einsatzbereiche wären das Online-Banking und Online-Shopping mit einem Zuspruch von 38 beziehungsweise 33% unter den Internet-Nutzern.
- Die Zahlungsbereitschaft für das Personalausweis-Kartenlesegerät war eher gering, fast die Hälfte der befragten Personen gab an, das Gerät nur zu nutzen, wenn es kostenlos wäre beziehungsweise bis zu 10€ kosten würde.

Es zeigt sich, dass die Bevölkerung dem neuen Personalausweis bereits vor Einführung kritisch gegenüberstand, eine Beobachtung, die durch eine Erhebung aus dem Jahr 2012 auch für die Folgejahre belegt werden kann. Anfang 2011, etwa 3 Monate nach der Umstellung, wurden bereits etwa 1,1 Millionen neue Personalausweise ausgegeben. Etwa die Hälfte aller Antragssteller haben dabei die Online-Ausweisfunktion freischalten lassen, die für die tatsächliche Nutzung nötige Software wurde bis zu dem Zeitpunkt allerdings lediglich 29.000 runtergeladen[61]. Die Akzeptanz hat sich in den Folgejahren tendenziell sogar eher weiter verschlechtert: So hatten innerhalb von zwei Jahren nach seiner Einführung etwa 17 Millionen Bundesbürger den neuen Personalausweis angefordert, die Online-Ausweisfunktion haben dabei jedoch lediglich 5 Millionen und somit nicht einmal ein Drittel der Antragssteller aktivieren lassen[62]. Auch in 2013 konnte keine merkliche Steigerung der Nutzung der Authentisierungsfunktion festgestellt werden[63].

[60] Vgl. BITKOM (2010)
[61] Vgl. Sietmann, R. (2011)
[62] Vgl. CSC (2012)
[63] Vgl. Reiter, A. (2013)

Gründe für die mangelnde Akzeptanz sind vielseitig. Die Bundeszentrale für politische Bildung (bpb) argumentiert, dass Sicherheitslücken wohl eher zu vernachlässigen seien, da „Internetnutzerinnen und –nutzer Einfachheit höher bewerten als technische Sicherheit.“[64] Stattdessen gelten vor allem die bisher geringe Anzahl an Einsatzgebieten sowie die lückenhafte Aufklärung als Hauptfaktoren. 2012 verfügten so lediglich 129 Unternehmen und Behörden über ein entsprechendes Berechtigungszertifikat, um die Daten für das Online-Ausweisverfahren vom Personalausweis auszulesen[65]. Auch Bundes-CIO (Chief Informational Officer) Cornelia Rogall-Grothe führt an, dass die Nutzung der Online-Ausweisfunktion sowohl für den Bürger als auch für die Unternehmen noch neu sei und die bisherige Freischaltung „doch bereits eine beachtliche Zahl“[66] sei. Damit verbunden ist auch der Aspekt der fehlenden Bekanntheit der Möglichkeit des Online-Ausweisens. Pablo Mentzinis, Bereichsleiter des Public Sectors der BITKOM, bemängelt in diesem Zusammenhang die Aufklärung bei den Behörden vor Ort: Die Verwaltung in den kommunalen Meldeämtern rate sogar von der Aktivierung der eID ab, anstatt das Angebot zu verbreiten[67].

Wie die Eingangsstudie der BITKOM ergeben hat, könnte ein weiterer ausschlaggebender Punkt der Kostenfaktor für das Kartenlesegerät sein. Man unterscheidet hier zwischen drei verschiedenen Kategorien: Basis-, Standard- und Komfortleser, die sich in ihren Funktionalitäten und damit auch im Preis unterscheiden[68]. Basisleser ohne Display und Tastatur sind schon ab 20€ erhältlich, für den Standardleser mit integrierter Tastatur zur PIN Eingabe liegt man bei etwa 70€ und der Komfortleser schließlich, der zusätzlich über ein Display verfügt und die Unterschriftsfunktion unterstützt kostet rund 160€[69]. Wie anfangs aufgezeigt, hat die Studie allerdings ergeben, dass ein Großteil der Bevölkerung nicht bereit wäre, mehr als 10€ für ein entsprechendes Gerät auszugeben.

Trotz all dieser Aspekte, schätze ein Sprecher des Bundesinnenministeriums die bisherige Verbreitung in der Bevölkerung für „nicht ungewöhnlich“ ein, da „[vergleichbare] Entwicklungen in der Vergangenheit zeigen, dass sich technische Lösungen anfangs zunächst langsam entwickeln und erst Jahre später vollends durchsetzen.“[70] Auch Rogall-Grothe zeigt sich zuversichtlich, dass die Akzeptanz in der nächsten Zeit mit zunehmenden Anwendungsmöglichkeiten steigen wird. Ihrer Meinung nach, wird sich die Online-Ausweisfunktion durchsetzen, sobald die Behörden auf Länder- und Kommunalebene sicherstellen, „dass Bürger und Unternehmen diese Wege zu einem einfachen elektronischen Zugang zur Verwaltung auch

---

[64] Kubicek, H. (2011)
[65] Vgl. CSC (2012)
[66] Reiter, A. (2013)
[67] Vgl. Hengl, H. (2012)
[68] Vgl. Bundesministerium des Innern (2013h)
[69] Vgl. Kämmer, A. (o. J.)
[70] Hengl, H. (2012)

gehen können und flächendeckend die Nutzung von […] eID-Funktion anbieten.“[71] Laut ihrer Aussage wird derzeit auch bereits an neuen Lösungen gearbeitet, „etwa in Verbindung mit Smartphones und Tablet-PCs“[72]

Es gibt bereits Positivbeispiele, die diese Thesen stützen:[73] Die Städte Münster und Ingolstadt etwa gelten als Vorbilder, da hier das Online-Verfahren aktiv eingesetzt und von den Bürgern auch willkommen genutzt wird. Ebenso kann die Deutsche Kreditbank anhand der hohen Weiterempfehlungsquote belegen, dass ihre Kunden das Legitimationsverfahren begrüßen, das ihnen erlaubt, online ein Konto samt Kreditkarte zu beantragen. Auch in der Versicherungsbranche findet die Online-Ausweisfunktion bereits Anwendung. So stützt sich die Gothaer Versicherung bei der Beantragung von Kfz-Versicherungen auf die Online-Authentisierungsfunktion.

Alles in allem bleibt festzuhalten, dass die bisherige Akzeptanz in der Bevölkerung zwar noch verhältnismäßig gering ist, der allgemeine technologische Fortschritt sowie die Weiterentwicklung der Online-Ausweisfunktion die Verbreitung der eID jedoch stetig fördern. Dabei lautet die vorherrschende Meinung, dass mit einer besseren Aufklärung der Bürger auch die Nutzung der neuen Möglichkeiten einhergehen wird.

2.4 Der eID Server

Wie in Kapitel 2.1 erwähnt, ist bei dem Anbieten der Online-Ausweisfunktion aus Unternehmenssicht zu beachten, dass es aus Sicherheitsgründen über einen sogenannten eID Server verfügen muss. Entscheidet sich ein Unternehmen also für den Einsatz der elektronischen Authentisierung, so ist neben der technischen Implementierung innerhalb der eigenen Website demnach auch unbedingt der Aufwand für diesen eID-Server zu berücksichtigen.

Zum Verständnis ist hier ein Blick auf die Funktionsweise des elektronischen Identifizierungsverfahrens notwendig.

[71] Reiter, A. (2013)
[72] Ebenda
[73] Hengl, H. (2012)

Abb. 2: Kommunikationswege im elektronischen Identifizierungsverfahren[74]

Soll das eID-Verfahren genutzt werden, wird zwischen der Website des Unternehmens und dem eID-Client des Kunden (also beispielsweise der AusweisApp oder der BürgerApp) noch ein Verbindungsstück in Form eines eID-Servers benötigt.

Dieser garantiert gegenüber dem eID-Client des Kunden, dass es sich wirklich um das Unternehmen handelt, das gerade auf der Website angibt, die Daten abzufragen. Gleichzeitig überträgt der eID-Server die vom Kunden abgefragten Daten in verschlüsselter Form zum Server des Unternehmens, von welchem die Website gehostet wird. Der Einsatz eines eID-Servers ist also zwingend notwendig.

Ein eID-Server kann vom Unternehmen auf verschiedene Wege realisiert werden. Der eID-Server kann:

- vom Unternehmen selbst aufgebaut werden.
- bei einem anderen Unternehmen gehostet und die Nutzung eingekauft werden.
- in Form eines eID-Service eingekauft werden, sodass die gesamte technische Umsetzung zwischen Unternehmens-Website und eID-Client des Kunden ausgelagert wird.

[74] Der e-ID-Client (2013)

Die einzelnen Möglichkeiten bieten verschiedene Vor- und Nachteile, auf die im Folgenden kurz eingegangen werden soll.

Aufbau eines eigenen eID-Servers

Entscheidet sich ein Unternehmen für diese Variante, so genießt es im Betrieb die größtmögliche Flexibilität und ist über das Level an Datenschutz immer im Bilde. Allerdings enthält diese Option sehr große Einstiegshürden, da der Aufbau und Betrieb eines eID-Servers sehr komplex und kostenintensiv ist.

So muss der eID-Server in einer geschützten Umgebung betrieben werden und darf nur vom BSI zertifizierte Komponenten enthalten. Vor Inbetriebnahme muss der Server zudem durch das BSI abgenommen werden. Außerdem muss vom Unternehmen selbst sichergestellt werden, dass der eID-Server mit dem eID-Client des Kunden kommunizieren kann, weshalb die technische Richtlinie BSI TR-03130[75] erfüllt sein muss.

Einkauf von Nutzungsrechten für einen eID-Server

Verschiedene Anbieter haben bereits eID-Server in Betrieb, die gegen ein Entgelt genutzt werden können. Hierbei entgeht das Unternehmen dem Aufwand der Einrichtung und des Betriebs des eID-Servers, muss jedoch selbst für eine technische Anbindung an die eigene Website sorgen und sich um die Software auf dem eID-Server kümmern.

Angeboten wird ein eID-Server unter anderem von den folgenden Unternehmen:

- AGETO Service GmbH
- OpenLimit SignCubes GmbH
- media transfer AG
- bremen online services GmbH& Co. KG (BOS)

Nutzung eines eID-Services

Diese Variante ist für das Unternehmen die komfortabelste, da sich der Dienstanbieter um die gesamte Einrichtung und Betreuung des eID-Servers und um sämtliche Anbindungen kümmert.

Jedoch muss berücksichtigt werden, dass die Nutzung eines solchen Services mit erheblichen Kosten verbunden ist und zusätzlich in diesem Fall eine Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz zustande kommt.

[75] Bundesministerium für Sicherheit in der Informationstechnik (o.J. i)

Letzteres enthält das Risiko, dass das Unternehmen für die Einhaltung und Überwachung der Sicherheitsvorschriften beim Service-Provider verantwortlich ist und beispielsweise im Falle eines Daten-Lecks haftbar gemacht werden kann.

Unter anderem haben folgende Anbieter eID-Services in ihrem Portfolio:

- Bundesdruckerei GmbH
- bremen online services GmbH& Co. KG (BOS)
- DataClearing NRWciteq - Informationstechnologie für Kommunen (Stadt Münster) & Kommunales Rechenzentrum Niederrhein (KZRN)
- Deutsche Post Com GmbH, Geschäftsfeld Signtrust
- FUJITSU TECHNOLOGY SOLUTIONS GmbH
- media transfer AG
- Siemens IT Solutions and Services GmbH
-]init[AG für Digitale Kommunikation[76]

[76] Vgl. Die eID-Funktion (o.J.)

3 Die „AusweisApp“

Die AusweisApp unterstützt die Funktionen des neuen Personalausweises, mit dessen Hilfe sich der Bürger seit November 2010 im Internet ausweisen kann. Bei der Nutzung des neuen Personalausweises zur Kommunikation zum Beispiel mit Bürgerdiensten oder Versicherungen, muss sich auch der Geschäftspartner durch ein Berechtigungszertifikat für den angefragten Dienst ausweisen.[77] Die AusweisApp stellt hierbei die Verbindung zwischen dem benötigten Kartenlesegerät, dem Personalausweis und dem Geschäftspartner dar und gewährleistet den verschlüsselten und sicheren „Datenaustausch zwischen Personalausweis und Diensteanbieter“[78]. Es handelt sich bei der AusweisApp um eine kostenlose Softwareapplikation, welche die Betriebssysteme Windows, Linux und Mac OS unterstützt.[79]

Der Prozess des Online-Ausweisens funktioniert „sehr einfach“[80]. Der Nutzer sieht in einer Übersicht, welche der auf dem Personalausweis gespeicherten Daten der Geschäftspartner benötigt. Dabei gilt das Prinzip der Datensparsamkeit, denn nur die notwendigen Daten werden dem Anbieter nach Einverständnisprüfung des Bürgers übermittelt. Die Abfrage des Einverständnisses erfolgt mittels einer sechsstelligen PIN, welche für den Nutzer einmalig generiert wurde. Gleichzeitig wird geprüft, ob der Personalausweis gültig und nicht gesperrt ist. Zudem wird die Existenz eines staatlichen Berechtigungszertifikats auf Seiten des Anbieters kontrolliert. Diese beiden Prüfungen werden auf einem eID-Server ausgeführt, auf welchen der Anbieter keinen Zugriff hat. Somit wird ausgeschlossen, dass der Anbieter auf die Daten des Personalausweises aktiv zugreifen kann.[81]

Die Sicherheitsmaßnahmen im Datenschutz sind bei der Nutzung der AusweisApp „auf dem höchsten Niveau“[82], was durch die Prinzipien der Datensicherheit und der Datensparsamkeit gewährleistet wird. Auf diese wird im weiteren Verlauf der Arbeit Bezug genommen.

3.1 Ressourcenanforderungen und Komptabilität

Um die AusweisApp nutzen zu können, wird sowohl ein internetfähiger PC mit kompatiblem Betriebssystem und Browser als auch ein geeignetes Kartenlesegerät benötigt. Im Folgenden werden die Anforderungen im Detail erklärt.

---

[77] Vgl. Bundesministerium des Innern (2013n)
[78] Bundesministerium des Innern (2013o)
[79] Vgl. AusweisApp-Portal (o.J. b)
[80] Bundesministerium des Innern (2013p)
[81] Vgl. Bundesministerium des Innern (2013n)
[82] Ebenda

3.1.1 Betriebssystem

Nach Angaben des Herstellers unterstützt die AusweisApp folgende Betriebssysteme:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Ubuntu 12.04 / 32bit
- Ubuntu 12.10 / 32bit
- Ubuntu 13.04 / 32bit
- Debian 6.0 / 32bit
- openSUSE 12.1 / 32bit
- openSUSE 12.2 / 32bit
- openSUSE 12.3 / 32bit
- Mac OS X 10.6
- Mac OS X 10.7
- OS X 10.8[83]

Auffällig ist hier, dass zwar alle Windows-Versionen unterstützt werden, die AusweisApp jedoch bislang nicht für Mac OS X 10.9 angepasst wurde.[84] Obwohl die Beta-Version des neuen OS X bereits seit den Sommermonaten zur Verfügung steht, scheint es den Entwicklern noch nicht gelungen zu sein, die nötigen Anpassungen vorzunehmen. Die Versionshistorie bestätigt dies und zeigt die letzte Anpassung der AusweisApp für Mac OS X im Juli 2013.[85]

Bei den Versionen für Ubuntu ist zu beachten, dass keine Anpassung für 64-bit Systeme vorgenommen wurde, sodass Benutzer solcher Systeme ebenfalls die 32-bit Variante nutzen müssen.

3.1.2 Browser

Nach Herstellerangaben können folgende Browser verwendet werden: [86]

- Den Microsoft Internet Explorer (32 Bit) ab Version 6 (Windows Betriebssysteme)
- Mozilla Firefox Version 17
- iceweasel ab Version 3

---

[83] Vgl. AusweisApp-Portal (o.J. c)
[84] Vgl. Donath, A. (2013)
[85] Vgl. AusweisApp-Portal (o.J. d)
[86] Vgl. AusweisApp-Portal (o.J. e)

Hierbei gibt es jedoch auch Einschränkungen. So wird Mozilla Firefox gegenwärtig nur in der Version 17 Extended Support Release (ESR) unterstützt[87], obwohl Mozilla mittlerweile bereits Version 26 vertreibt.[88]

Ebenso ist laut Hersteller die Ausweis-App mit Internet Explorer 9 nicht ohne die Installation eines zusätzlichen Add-ons nutzbar. Zudem wird die Funktion „InPrivate-Browsen“ nicht unterstützt, welche vermeidet, dass Browserverlauf, temporäre Internetdateien, Formulardaten, Cookies, Benutzernamen und Kennwörter gespeichert werden.[89]

Darüber hinaus ist anzumerken, dass die AusweisApp weder mit Safari noch Google Chrome nutzbar ist. Diese beiden Browser kommen gemeinsam auf fast 50% Marktanteil in Deutschland, wodurch eine sehr große Gruppe der möglichen AusweisApp-Nutzer zur Installation eines weiteren Browsers gezwungen würde.

Abb. 3: Aktuelle Browser-Statistik für Deutschland[90]

Die Unterstützung dieser beiden Browser ist laut Hersteller nicht möglich, da die in Safari und Google Chrome verwendete Sandbox-Technologie eine Kommunikation zwischen Browser, AusweisApp, eID-Server und Webdienst unterbindet.[91]

[87] Vgl. AusweisApp-Portal (o.J.e)
[88] Vgl. Humpa, M. (o.J.)
[89] Vgl. Windows (o.J.)
[90] Vgl. Browser-Statistik (2013)
[91] Vgl. AusweisApp-Portal (o.J.e)

3.1.3 Kartenlesegerät

Zusätzlich zu einem geeigneten PC mit passend konfiguriertem Browser wird ein Kartenlesegerät benötigt, um die Ausweisdaten mit dem PC auslesen zu können.

Die hierfür geeigneten Geräte können alle über die Website der AusweisApp gefunden werden[92] und zeichnen sich durch eine Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) aus.[93]

Wie im zweiten Kapitel erwähnt, werden Kartenlesegeräte in unterschiedlichen Ausführungen angeboten, wobei schon die Standard-Kartenlesegeräte ausreichend sind, um sich mit dem neuen Personalausweis im Internet identifizieren zu können. Während die Standard-Kartenlesegeräte über keine eigene Tastatur verfügen, kann in höherwertigen Varianten die zum Ausweis gehörige PIN direkt über eine im Gerät eingebaute Tastatur eingegeben werden. Hierdurch soll verhindert werden, dass die persönliche PIN über Tastatur-Überwachungstools aufgezeichnet werden kann.

High-end-Produkte bieten neben einer eingebauten Tastatur ebenfalls ein Kryptographiemodul mit Display, welches die Generierung einer elektronischen Signatur ermöglicht.

3.2 Sicherheitsaspekte

Um einen umfassenden Eindruck zum Thema Sicherheit bei der AusweisApp gewinnen zu können, ist die Betrachtung mehrerer Aspekte erforderlich. Insgesamt gibt es vier Faktoren, die Einfluss auf die Sicherheit haben und potentielle Ansatzpunkte für Kriminelle bieten, die an die Ausweisdaten gelangen wollen. Diese vier Faktoren sind die AusweisApp an sich, der Computer, auf welchem die AusweisApp installiert ist, das Kartenlesegerät und zuletzt der Nutzer selbst. Im Folgenden sollen diese Faktoren im Hinblick auf technische Schutzmaßnahmen und etwaige Sicherheitslücken untersucht werden. Dabei ist zu beachten, dass die Aspekte Computer, Kartenlesegerät sowie Nutzer von allgemeiner Gültigkeit sind und nicht explizit für die AusweisApp gelten.

3.2.1 Computer

Der Anwender-PC, auf dem die AusweisApp läuft, um die elektronische Identifizierung durchzuführen, bietet das erste potentielle Ziel für Angreifer von außen.

---

[92] Vgl. AusweisApp-Portal (o.J. f)
[93] Vgl. AusweisApp-Portal (o.J. g)

Ein ausreichender Schutz des PCs ist an sich leicht zu erreichen, jedoch durch Unkenntnis und Nachlässigkeit oft nicht vorhanden. Aus diesem Grund versucht das Bundesamt für Sicherheit in der Informationstechnik seit einiger Zeit, den Bürgern genau dieses Risiko bewusst zu machen und Wege aufzuzeigen, wie die Gefahr eines unerlaubten, externen Zugriffs auf den eigenen PC vermieden werden kann.

So hat das BSI auf seiner Website eine eigene Rubrik geschaffen, die auf einfache und verständliche Weise versucht, den Bürgern Wissen über grundlegende Sicherheitsmechanismen zu vermitteln.[94]

Um eine ausreichende Sicherheit auf dem eigenen PC zu gewährleisten, empfiehlt das BSI Dinge wie eine regelmäßige Aktualisierung von Virenschutz und Firewalls, die Durchführung von Sicherheitsupdates, Verschlüsselung der Kommunikation, die Erstellung von Sicherheitskopien und der regelmäßige Wechsel von Passwörtern.[95]

Durch derartige Maßnahmen kann bereits eine Vielzahl möglicher Angriffe von außen verhindert werden, beispielsweise ist es so nahezu unmöglich, Viren oder Malware auf den Anwender-PC einzuschleusen.

Darüber hinaus gibt das BSI umfangreiche Tipps zur Erstellung sicherer Passwörter, da zu simple Kennwörter mithilfe automatisierter Software leicht herausgefunden werden können. Um dies zu vermeiden, sollten Passwörter immer gewissen Standards wie einer ausreichenden Zeichenlänge und dem Einsatz von Sonderzeichen entsprechen.[96]

Obwohl die Sicherheit des eigenen Computers jedem Anwender ohnehin ein Anliegen sein sollte, zeigt sich in der Realität, dass dieses Thema an vielen Stellen zu kurz kommt. So belegen Studien beispielsweise, dass über 40% der Wireless Local Area Netzwerke (WLAN) in Deutschland nicht ausreichend gesichert sind.[97] Aus Gründen dieser Art rät auch eine vom BSI in Auftrag gegebene Studie dringend zur Schaffung eines Bewusstseins zum Thema Sicherheit bei den Anwendern, da durch den Einsatz der elektronischen Ausweisfunktion rechtsverbindliche Geschäfte getätigt werden können und ein Missbrauch dieser Funktion daher auch schwerwiegendere Konsequenzen haben kann.[98]

[94] Vgl. Bundesamt für Sicherheit in der Informationstechnik (o.J. c)
[95] Vgl. Bundesamt für Sicherheit in der Informationstechnik (o.J. d)
[96] Vgl. Bundesamt für Sicherheit in der Informationstechnik (o.J. e)
[97] Vgl. Hamburger Abendblatt (2009)
[98] Vgl. Dietrich, C./Rossow, C./Pohlmann, N. (2010a)

3.2.2 Kartenlesegerät

Neben dem Anwender-PC bietet auch das für die elektronische Identifizierung verwendete Kartenlesegerät Möglichkeiten für Angreifer von außen, die Identifizierungsfunktion für unerlaubte Zwecke zu nutzen. Diese Sicherheitsrisiken sind allerdings mit relativ niedrigem Aufwand auch durch Anwender mit geringen Kenntnissen in der Informationstechnologie (IT) zu vermeiden, indem zwei wichtigen Aspekte Aufmerksamkeit geschenkt wird.

Zum einen sollte beim Kauf eines Kartenlesegeräts unbedingt darauf geachtet werden, dass dieses vom BSI für den Einsatz bei elektronischen Identifizierungsverfahren zertifiziert ist. Eine Liste der zertifizierten Geräte stellt das BSI auf der Website der AusweisApp zur Verfügung.[99]

Ein zertifiziertes Kartenlesegerät ist zwar keine Voraussetzung, um die AusweisApp nutzen zu können, jedoch empfiehlt es sich, beim Kauf auf das Zertifikat zu achten, da hierdurch davon ausgegangen werden kann, dass der Kartenleser über entsprechende technische Standards und Schutzfunktionen verfügt, um ein sicheres Ausweisen im Internet gewährleisten zu können.

Der Zertifizierung zugrunde liegt die technische Richtlinie 03119, welche Module auflistet, die je nach Kategorie des Kartenlesers verpflichtend oder optional zu verwenden sind.[100] Die Richtlinie lässt sich auf der Seite des BSI online einsehen.[101]

Neben der Zertifizierung sollte beim Kauf darauf geachtet werden, dass es sich mindestens um ein Standardlesegerät mit Tastatur handelt. Die Nutzung eines Basislesegeräts ist aus Sicherheitsgründen nicht anzuraten.

Grund hierfür ist, dass bei Basislesegeräten, im Gegensatz zu Standard- und Komfortlesegeräten, die PIN nicht direkt auf dem Gerät eingegeben werden kann, sondern über die normale Computertastatur eingetippt werden muss. Dies ermöglicht Angreifern von außen mithilfe sogenannter „Keylogger“-Programme die Tastatureingaben des Anwenders aufzuzeichnen und somit an die PIN zu gelangen.

Bei Standard- und Komfortlesegeräten lässt sich diese Gefahr durch eine im Lesegerät eingebaute Tastatur problemlos vermeiden, weswegen sowohl Hersteller von Lesegeräten[102],

[99] Vgl. AusweisApp-Portal (o.J. f)
[100] Vgl. TÜV Informationstechnik GmbH (o.J.), S. 11
[101] Vgl. Bundesamt für Sicherheit in der Informationstechnik (o.J.)
[102] Vgl. Spiegel Online (2011)

als auch eine vom BSI in Auftrag gegebene Studie deutlich vor dem Einsatz von Basis-Lesegeräten warnen.[103]

3.2.3 AusweisApp

Die AusweisApp verfügt über eine Reihe technischer Schutzmaßnahmen, jedoch gibt es auch einige sicherheitsrelevante Aspekte, die als kritisch zu bewerten sind.

Zunächst wurde von den Verantwortlichen beschlossen, den Source Code der AusweisApp nicht offen zu legen, um Angreifern von außen ein mögliches Eindringen in das Programm zu erschweren. Kritiker weisen allerdings daraufhin, dass daher zunächst auch etwaige Fehler unentdeckt bleiben, die unabhängige Tester sonst hätten finden können.[104]

Das Kommunikationsmodell der AusweisApp wurde in einer vom BSI in Auftrag gegebenen Studie inzwischen für gut befunden, nachdem Fehler beseitigt wurden, die in der ersten Version der AusweisApp noch enthalten waren. Hier war es noch möglich, über ein sogenanntes „Session-Hijacking" nach erfolgter Authentifizierung die Session von außen zu übernehmen. Dieser Angriffspunkt wurde mittlerweile jedoch behoben, wodurch es in diesem Bereich nun keine Sicherheitsbedenken mehr gibt.[105]

Bedenklicher hingegen ist das Thema Cookies in Verbindung mit der AusweisApp. So ist es dem Anwender nicht möglich, die AusweisApp zu nutzen, so lange Cookies deaktiviert sind. Der eigentliche Sicherheitsgewinn, der durch die Deaktivierung von Cookies entsteht, kann hier also nicht genutzt werden. In Tests, die von der Stiftung Warentest durchgeführt wurden, gab es keinerlei Möglichkeit, den Gebrauch von Cookies zu umgehen.[106] Durch den Einsatz dieser entstehen unter Umständen neue Möglichkeiten für Angreifer, über den Anwender-PC mittels Malware die Informationen aus den Cookies auszulesen.

Das massivste Risiko in Hinblick auf das Thema Rechtssicherheit ergibt sich bei der AusweisApp durch die fehlende Zertifizierung. In der neuen Personalausweisverordnung ist gesetzlich geregelt, dass eine Software, mithilfe derer eine Identifikation im Internet erfolgen kann, vom BSI zertifiziert werden muss. Allerdings wurde die AusweisApp trotz mehrerer Ankündigungen bis heute nicht zertifiziert. Nach Aussage des BSI wurde diese Zertifizierung bisher nicht vorgenommen, da *„aufgrund der Browser-Abhängigkeit der AusweisApp regelmäßige technische Anpassungen und Weiterentwicklungen (z.B. Browser-Plugins) unver-*

[103] Vgl. Dietrich, C./Rossow, C./Pohlmann, N. (2010b), S. 5
[104] Vgl. Schejbal, J. (2011)
[105] Vgl. Dietrich, C./Rossow, C./Pohlmann, N. (2010c), S. 9
[106] Vgl. Stiftung Warentest (2011)

meidbar waren.“ [107] Weiter erklärt das BSI, dass die AusweisApp trotzdem genutzt werden kann und keine Bedenken in Hinblick auf die Rechtssicherheit nötig seien.[108]

Allerdings rügt der Bundesrechnungshof in einer Bemerkung zum Jahresbericht 2012 das BSI für die fehlende Zertifizierung und hält Haftungsrisiken bei den Ausweisinhabern für nicht ausgeschlossen.[109]

3.2.4 Der Anwender

Zuletzt muss erwähnt werden, dass dem Anwender selbst beim Thema Sicherheit eine erhebliche Rolle zukommt und dieser sich nicht nur auf die Sicherheitsmechanismen der Technik verlassen darf.

Wie bereits beschrieben, sollte sich der Anwender zunächst umfassend informieren, bevor er ein Kartenlesegerät kauft und seinen Computer auf ein entsprechendes Sicherheitsniveau bringen. Erst nachdem dies geschehen ist, ist der Einsatz der Online-Ausweisfunktion überhaupt empfehlenswert.

Entschließt sich der Anwender zur Nutzung dieser Funktion, so sollte er grundlegende Dinge beachten, wie beispielsweise seinen Ausweis nach Benutzung vom Lesegerät zu nehmen oder seine PIN geheim zu halten. Nur so kann sichergestellt werden, dass Angreifer, die den Computer mit Malware infiziert haben, keinen unbemerkten Zugriff auf den Ausweis und die damit verbundenen Möglichkeiten erhalten.

Darüber hinaus ist auch ein Einsatz des eigenen Ausweises an fremden Computern nicht zu empfehlen, da die dortigen Sicherheitsmaßnahmen nicht bekannt sind. Nur wenn der Anwender sicher sein kann, dass der verwendete Computer auf dem neuesten Stand der Technik in Hinblick auf die Sicherheit ist, sollte dieser verwendet werden.

Erst wenn beim Anwender das im Text bereits angesprochene Bewusstsein für die Sicherheit seines Computers geschaffen wurde, sollte die elektronische Ausweisfunktion genutzt werden. Dass dies in vielen Fällen nicht der Fall ist, zeigt auch eine Studie des Sicherheits-Unternehmens F-Secure, nach der nur etwa 13% der PCs sicherheitstechnisch auf dem aktuellen Stand sind.[110]

Hier sollte sich jeder Anwender zunächst selbst fragen, ob er über das nötige technische Verständnis verfügt, um bedenkenlos von der elektronischen Ausweisfunktion Gebrauch zu machen.

---

[107] Vgl. AusweisApp-Portal (o.J.h)
[108] Vgl. ebenda
[109] Vgl. Heise online (2013)
[110] Vgl. Anti-Botnet Beratungszentrum (2013)

3.3 Benutzerfreundlichkeit

Im Jahr 2012 hat das Hasso-Plattner-Institut (HPI) für Softwaresystemtechnik im Auftrag des Bundesministeriums des Innern eine Studie zur Benutzerfreundlichkeit und Nutzungsfrequenz der AusweisApp durchgeführt. Das Ziel dieser Untersuchung hat darin bestanden, mögliche Verbesserungen zu erkennen, um den Nutzungsgrad der Online-Funktion des neuen Personalausweises zu steigern. Im Rahmen der Studie sind Befragungen zum Wissensstand und der Zufriedenheit der Nutzer durchgeführt worden und Beobachtungen und Interviews im Umgang mit der AusweisApp getätigt worden. Auf diesen Ergebnissen basierend hat das HPI Verbesserungsvorschläge entwickelt, welche die Benutzerfreundlichkeit und Akzeptanz der AusweisApp steigern können.[111]

Einhergehend mit der Akzeptanz der Bevölkerung für diese Technik ist der Mehrwert, den sie liefert. „Wichtig sind dabei auch subjektiv wahrgenommene Faktoren wie Sicherheit oder Vertrauen.“[112] Die AusweisApp sollte selbsterklärend zu bedienen sein und eine vertrauensvolle Bedienbarkeit signalisieren.

Das HPI hat Interviewpartner und Testpersonen im Alter zwischen 16 und 73 Jahren ausgewählt. Die durchgeführte Studie stützt sich auf 74 Interviews (inklusive 12 Experteninterviews) und 36 Tests. Im Fokus stand die Altersgruppe von 20 bis 30 Jahren. Das Team um die Untersuchung hat die Teilnehmer nach Zielgruppen zusammengestellt, wobei die folgenden sieben Gruppen identifiziert werden können:

- Bürger
- Studenten
- IT-Experten
- Eltern
- Pädagogen
- Akademiker
- Politiker

Die Gruppe der Experten wird durch Personen vertreten, die an Institutionen beschäftigt sind, welche eine aussagekräftige Verbindung zum neuen Personalausweis besitzen. Es handelt sich hierbei um das Bundesministerium des Innern, die Bürgerämter Potsdam und Berlin, das Fraunhofer Kompetenzzentrum neuer Personalausweis, die Bundesdruckerei sowie das Bundesverwaltungsamt.

[111] Vgl. Asheuer, J. et al. (2011)
[112] Ebenda

Um die Eindrücke, Erfahrungen, Wünsche und Ideen der Nutzer geordnet zu erfassen, hat das HPI einen Interviewleitfaden erarbeitet, welcher mit jeder Testperson abgearbeitet wird. Der Leitfaden beinhaltet viele Themengebiete zum neuen Personalausweis, wie zum Beispiel den Prozess der Ausweisbeantragung und –abholung oder zur Sicherheit und zum Vertrauen in diese Technologie. An dieser Stelle steht jedoch die Benutzerfreundlichkeit der AusweisApp und der Online-Ausweisfunktion im Mittelpunkt, weshalb lediglich die Ergebnisse dieser Teile vorgestellt werden.

„Die AusweisApp war einem großen Teil der befragten Bürger unbekannt“[113], leitet die Studie ihr Fazit zur Befragung zur AusweisApp ein. Vielen Teilnehmern sei nicht bewusst gewesen, dass eine Software und ein Lesegerät nötig seien, um von der Online-Funktion des neuen Personalausweises Gebrauch machen zu können. Das technische Verständnis für die Funktionen der AusweisApp sei oft nicht vorhanden gewesen. Einige der befragten Bürger haben die Erwartung vertreten, dass die AusweisApp mögliche Anwendungsfälle darstellt.

Weiterhin sind die Bürger in der Studie zur Online-Ausweisfunktion befragt worden. Hier lässt sich feststellen, dass der „Nutzen und Mehrwert der Online-Ausweisfunktion“[114] bisher nicht zu identifizieren gewesen sei. So zeigt das Ergebnis, dass keine der Testpersonen in der Lage war, Dienste zu nennen, welche die Online-Ausweisfunktion zur Verfügung stellt. Stattdessen herrschte teilweise die Annahme vor, dass man künftig mit Hilfe des neuen Personalausweises Zahlungen im Internet einfacher tätigen könne. Der Zustand dieser Unaufgeklärtheit ist auf unzureichende Erläuterungen auf den Bürgerämtern zurückzuführen. Die Studie ergab, dass selbst viele Mitarbeiter negativ gegenüber der Online-Ausweisfunktion des neuen Personalausweises eingestellt sind, da auch sie nicht ausreichend über dessen Nutzen und Mehrwert aufgeklärt sind.

Der zweite Teil des Tests zur Benutzerfreundlichkeit bestand aus Beobachtungen, die das HPI während der Nutzung und Bedienung der AusweisApp durchgeführt hat. Die Teilnehmer der Studie haben weiterhin an einer Befragung zu den Themen Nutzung, Funktionen, Verhalten und Gestaltung der Software teilgenommen. Der Fokus lag hierbei auf der Suche nach Informationen zur Online-Ausweisfunktion, der „Interaktion der Software“[115] und dem „Prozess der Ausweisaktivierung“[116]. Zusätzlich sind die Hilfestellung des Programms und der intuitive Umgang mit der Namensgebung der Funktionen untersucht worden. Der Anwendungstest ist mit den Versionen 1.7 und 1.8 für Windows XP/Windows Vista/ Windows 7 durchgeführt worden.

---

[113] Asheuer, J. et al. (2011)
[114] Ebenda
[115] Ebenda
[116] Asheuer, J. et al. (2011)

Da viele Teilnehmer der Studie die Online-Ausweisfunktion nicht freigeschaltet haben, wurden diese mit Testausweisen ausgestattet und haben den benötigten PIN-Brief, eine Broschüre mit Informationen und ein Lesegerät erhalten. In dieser Arbeit wird die Betrachtung des Studienergebnisses jedoch auf die Ausweis-Aktivierung und die wesentliche Nutzung beschränkt.

Außerdem wurde während der Testdurchführung die Verständlichkeit der Begriffe des Programms beobachtet. Hierbei sind die Verantwortlichen des HPI zu dem Ergebnis gekommen, dass die Testpersonen Schwierigkeit mit dem Verständnis der folgenden Begriffe hatten: Zertifikat, Signatur, eID-Funktion, Online-Ausweisfunktion, AusweisApp, Integrity Tool, e-Card-Zertifikat, Vertrauensbasis, Plug-In, Screen-Reader, Customer Access Number (CAN), msi-Datei, ATR, Integrität (der Software), Authentizität (der Software), Unversehrtheit (der Software). Der Umstand, dass einige dieser Fachwörter Synonyme sind, verwirrte die Nutzer mehr, als dass sich daraus Klarheit ergab.

Viele der am Test Beteiligten vertraten die Erwartung, dass sie „kurze, selbsterklärende Anweisungen“[117] im Programm vorfinden, anhand derer sie die jeweils nächsten Schritte im Umgang mit der AusweisApp nachvollziehen können. Hier herrschte ein großes Missverständnis vor, da die Nutzer annahmen, es würde sich bei der AusweiApp um eine eigenständige Lösung mit aktiv nutzbaren Funktionen handeln.

Im Hinblick auf die Benutzerfreundlichkeit der AusweisApp lässt sich weiterhin feststellen, dass bereits bei der Beschaffung von Informationen und dem Download der Software erste Probleme auftauchten. Die Informationen in der Broschüre sind zu wenig auf die Bedürfnisse der Nutzer zugeschnitten. Außerdem hat diese ein anderes Design als die Internetseite der AusweisApp (ausweis.bund.de), was für Verwirrungen sorgte. Durch die bereitgestellten Informationen ist den Testpersonen das Zusammenwirken der beteiligten Institutionen nicht klar geworden. Zudem zeigt der Computer den Download der AusweisApp von der offiziellen Webseite ausweis.bund.de nicht als vertrauenswürdige Quelle an, was ebenfalls negativ empfunden wurde.

Ferner waren die Unterschiede der vielen erhältlichen Lesegeräte nicht erkennbar. Es sei hier aus den Erklärungen nicht erkennbar, welche Anforderungen ein Lesegerät zu erfüllen habe und warum bestimmte Modelle sicherer arbeiten sollten als andere. Die Nutzer hätten sich an dieser Stelle klare Abgrenzungen als Entscheidungshilfe gewünscht und eine Aufstellung der Geräte mit dem besten Preis-Leistungs-Verhältnis. Es lässt sich hierzu festhalten, dass die großen Preisunterschiede zwischen einzelnen Geräten für die Testpersonen nicht nachvollziehbar seien. In Zusammenhang mit diesem Aspekt steht die Tatsache, dass

[117] Asheuer, J. et al. (2011)

nirgendwo herausgestellt wird, wo Lesegeräte erworben werden können. Dies ist gerade für ältere Nutzer, die nicht mit Online-Shoppingportalen vertraut sind, ein Hindernis.

Auch die Installation der Software barg einige Schwierigkeiten. So tauchen hier im Laufe des Prozesses einige Begriffe auf, mit denen die Nutzer nichts anfangen konnten und die auch nirgendwo erklärt werden. Das Installationsarchiv, welches nach dem Entpacken der heruntergeladenen Datei zur Verfügung steht, birgt so viele Dateien, dass die Nutzer nicht wussten, welche Datei die Installationsdatei ist. Das hier verwendete Dateiformat *.msi war den Beteiligten nämlich nicht bekannt. Nach der Installation der AusweisApp muss der Nutzer erst ein umfassendes Software-Update durchführen, um die AusweisApp nutzen zu können. Dies wurde als störend empfunden, da die allgemeine Meinung vorherrschte, heruntergeladene Programme verfügten automatisch über die aktuellste Version. Wollten die Nutzer die heruntergeladene AusweisApp schließen, stellten sie erstmalig fest, „dass die Anwendung im Hintergrund als Prozess aktiv ist“[118] und nur über das entsprechende Symbol in der Status-Leiste ausgeschaltet werden kann.

Zur Aktivierung der AusweisApp lassen sich ebenfalls Kritikpunkte der vom HPI durchgeführten Studie nennen. Das Lade-Fenster der AusweisApp, welches sich nach Start des Programms öffnet, bleibt stets im Vordergrund, so dass an dieser Stelle keine weiteren Programme genutzt werden können. Nach der Fertigstellung des Ladens wird die AusweisApp in keinem Fenster geöffnet, wodurch der Nutzer keine Information darüber erhält, ob die Anwendung „erfolgreich gestartet wurde oder ein Problem vorliegt“[119]. Das Fehlen einer Benutzeroberfläche haben die Testpersonen als irritierend empfunden, da sie dies von anderen Softwareprodukten als Standard wahrnehmen. Über das sich in der Start-Leiste befindende Icon kann der Konfigurator geöffnet werden. Hier lässt sich jedoch lediglich die PIN verwalten. Es werden keine weiteren realen Funktionen bereitgestellt, was nach Ansicht der Testpersonen nicht ihren Erwartungen an die AusweisApp entspricht.

Bei der PIN-Aktivierung gibt es bei den an der Studie Beteiligten weitere Verwirrungen, da die Begrifflichkeiten irreführend verwendet werden. Die Bedienung der AusweisApp birgt hier großes Fehlerpotential, da die Buttons „PIN ändern“ und „PIN aktivieren“ bei der ersten Anwendung oft nicht eindeutig identifiziert werden konnten. Nach der erfolgreichen Änderung der PIN erhält der Nutzer keine Bestätigung für diesen Vorgang, was von den Testpersonen als verwunderlich zur Kenntnis genommen worden ist.

Es besteht die Möglichkeit, dass die PIN bei Abholung des Personalausweises im Bürgeramt gesetzt wird. Oft haben die Nutzer die Zahlenkombination jedoch bis zur ersten Verwendung

[118] Vgl. Asheuer, J. et al. (2011)
[119] Ebenda

der Online-Ausweisfunktion vergessen. Da die AusweisApp keinen Hinweis darauf gibt, ob ein PIN schon existiert oder nicht, haben die Testpersonen den Aktivierungscode aus dem Brief verwendet, worauf der Personalausweis nach drei falschen Eingaben und anschließender Verwendung der CAN gesperrt wird.

Ein großer Kritikpunkt ist der Prozess der Datenübermittlung. Hier werden die Daten abgefragt, die er dem Diensteanbieter übermitteln möchte und kann eine manuelle Änderung vornehmen. In diesem Fall werden die Daten jedoch nicht übertragen und der Dienst kann nicht Anspruch genommen werden, was die AusweisApp allerdings nur manchmal mit einer Fehlermeldung anzeigt. Die Nutzer fühlten sich hier um ihre Handlungsmacht stark betrogen. Außerdem sei ihnen nicht klar kommuniziert worden, warum und welche Daten von einem Anbieter benötigt wurden. Außerdem ist den Testpersonen während dieses Tests nicht klar geworden, wann die Datenübermittlung abgeschlossen war.

3.4 Administration

Im Zuge des Gebrauchs und der Nutzung der AusweisApp treten immer wieder Fragen und Probleme auf. Auf der Webseite ausweis.bund.de kann der Nutzer in einem bestehenden Portal zu häufigen Fragestellungen (engl. Frequently Asked Questions, FAQ) Hilfe finden. Hier gibt es Frage- und Antwortsammlungen zu den folgenden Themen:

- Allgemein
    - Update
    - Hilfe/Supportanfragen
    - Integritätsprüfung
    - Proxyfähigkeit
    - Start der Anwendung
    - Installation
    - Zertifizierung
- Betriebssysteme
- Browser
- Bekannte Probleme
- Karten
    - Neuer Personalausweis
    - Kartenaktivierung
- Kartenleser
- Sicherheit
- Online-Ausweisfunktion

- Barrierefreiheit
- Fehlermeldungen
- Portal www.ausweisapp.bund.de[120]

Unter der Rubrik Online-Ausweisfunktion finden sich so beispielsweise grundlegende Fragen zum Thema. Hier einige Beispiele:

- Wozu dient die Online-Ausweisfunktion?
- Wie werden Ihre persönlichen Daten bei der Online-Ausweisfunktion geschützt?
- Wozu können Sie die Online-Ausweisfunktion nutzen?
- Wie funktioniert die Online-Ausweisfunktion?
- Welche Hardware wird für die Online-Ausweisfunktion benötigt?[121]

Diese Fragen sind für den Nutzer der AusweisApp des neuen Personalausweises von großer Hilfe und werden jeweils in einigen präzisen Sätzen beantwortet.

Für den Fall, dass ein Nutzer ein Problem feststellt, welches nicht im FAQ-Katalog zu finden ist, steht ihm auf der Webseite ausweis.bund.de eine Supportfunktion zur Verfügung. Hier ist ein Webformular hinterlegt, in dem Probleme gemeldet, Wünsche geäußert und Fragen gestellt werden können.[122] Die Webseite verspricht, dass die Eingänge an Meldungen gesammelt und überprüft werden und anschließend bei der andauernden Weiterentwicklung der AusweisApp berücksichtigt werden. Negativ fällt bei der Verwendung des Webformulars auf, dass das Ausfüllen der Felder „aus technischen Gründen auf 10 Minuten begrenzt ist“[123].

Für weitere Fragen zur AusweisApp sollen sich Nutzer an das Bundesamt für Sicherheit in der Informationstechnik wenden. Die Kontaktdaten sind im Impressum der Internetseite aufgeführt.[124]

3.5 SWOT Analyse des Programms

Um die Ergebnisse der untersuchten Aspekte zur AusweisApp zusammenzufassen, wird eine SWOT-Analyse durchgeführt. Auf die zusammenfassende Übersicht in tabellarischer Form folgt eine kurze Erläuterung:

---

[120] Vgl. AusweisApp-Portal (o.J. c)
[121] AusweisApp-Portal (o.J. i)
[122] Vgl. AusweisApp-Portal (o.J. j)
[123] Ebenda
[124] Vgl. AusweisApp-Portal (o.J. k)

Interne Analyse	**Strenghts** – Offizielle Unterstützung und Finanzierung durch den Bund – Supportfunktionen für den Endanwender – Häufige Fragen wurden bereits geklärt und sind auf dem Portal verfügbar	**Weaknesses** – Eingeschränkte Kompatibilität mit Betriebssystemen und Browsern – Unzureichende Aufklärung – Sicherheitslücken durch Cookies – Gemindertes Vertrauen da Quellcode nicht offen zugänglich und Anwendung bereits gehackt wurde – Fehlende Zertifizierung – Umstrittene Benutzerfreundlichkeit durch ungeklärte Abkürzungen
Externe Analyse	**Opportunities** – Unterstützt eine Digitalisierung und schnellere Kommunikation – Möglichkeit, Geld und Zeit zu sparen – Verbesserungspotential durch Reaktion auf umfassende Studien	**Threats** – Unsichere Handhabung der Online-Ausweisfunktion durch Endanwender – Mangelnde Sicherheitsvorkehrungen auf dem PC des Nutzers – Basis-Kartenlesegeräte ermöglichen die Ermittlung der PIN

Strengths

Eine der bestehenden Stärken der AusweisApp ist ihre Unterstützung durch den Bund. Dank der finanziellen Mittel, die dem Entwicklungsteam zur Verfügung stehen, ist eine ständige Weiterentwicklung möglich; gleichzeitig können auch Gelder in die Supportfunktion für den Endanwender gesteckt werden. Das Entwicklungsteam der AusweisApp ist klar strukturiert, was gegebenenfalls das Vertrauen in die Anwendung steigert. Gleichzeitig findet der Endanwender durch ein Portal mit häufigen Fragen und deren Antworten Hilfe in der Nutzung der Applikation.

Weaknesses

Weitaus umfangreicheres als zu den Stärken der AusweisApp lässt sich derzeit zu deren Schwächen sagen. So beginnt die Liste mit der Kompatibilität der Betriebssysteme. Die AusweisApp steht dem Nutzer für die Betriebssysteme Windows, Linux und Mac zur Verfügung. Somit werden zwar die gängigsten Systeme abgedeckt, jedoch haben Bürger mit einem anderen Betriebssystem von Vornherein nicht die Möglichkeit, die Dienste der AusweisApp in Anspruch zu nehmen. Zudem ist anzumerken, dass die AusweisApp für Mac OS X 10.9 bislang nicht zur Verfügung steht und Ubuntu bisher nur in der 32-bit Variante erhältlich ist. Ähnlich verhält es sich mit der Browserkompatibilität. Die AusweisApp lässt sich in Verbindung mit den Browsern Microsoft Internet Explorer ab Version 6, Mozilla Firefox Version 17 und iceweasel ab Version 3 nutzen. Auch hier werden einige gängige Browser abgedeckt, in vielen Fällen muss jedoch für die Nutzung der AusweisApp ein neuer Browser gela-

den werden. Dies ist zum Beispiel bei der Nutzung der Browser von Safari und Google Chrome von Nöten, da diese nicht von der AusweisApp unterstützt werden.

Ein umstrittenes Thema der AusweisApp ist die Sicherheit. Sicherheitslücken der AusweisApp selbst resultieren daraus, dass der Source Code nicht öffentlich zugänglich ist. Daher können Fehler und Schwachpunkte des Programms nicht aufgedeckt werden, wodurch Schwachstellen nicht verbessert werden können und es sogar bereits zu einem erfolgreichen Angriff auf die Anwendung kam. Des Weiteren kann der Anwender die AusweisApp nicht nutzen, wenn Cookies deaktiviert sind, worin ein Defizit der Sicherheit für den Nutzer zu sehen ist. Der Aspekt, welcher hier am kritischsten zu bewerten ist, ist die fehlende Zertifizierung der AusweisApp durch das BSI, wodurch die Rechtssicherheit nicht einwandfrei geklärt ist.

Eine weitere Schwäche stellt die Benutzerfreundlichkeit der AusweisApp dar. Die Studie des HPI belegt, dass einer Großzahl der Nutzer die Notwendigkeit der AusweisApp nicht bewusst ist. Auch nach der Installation der Software sind viele verunsichert, wie genau das Programm genutzt wird und sind erstaunt, wenn sie feststellen, dass es lediglich aus einem Programm besteht, das im Hintergrund arbeitet und welches nicht aktiv vom Nutzer bedient werden kann. An dieser Stelle besteht noch viel Aufklärungsbedarf. Weitere Schwierigkeiten traten im Rahmen der Studie mit Begrifflichkeiten auf, die die Nutzer sich nicht selbst erklären konnten. Außerdem gab es Verwirrungen bei dem Download der AusweisApp, der PIN-Aktivierung und dem Prozess der Datenübermittlung.

Opportunities

Die große Chance der AusweisApp liegt vor allem in dessen Grundgedanken. Die Bürger bekommen durch die Nutzung der AusweisApp die Möglichkeit, ihre Daten einfacher zu verwalten und Dienste von Finanzinstitutionen, Versicherungen und Behörden in Anspruch zu nehmen. Auf diese Weise können sie Zeit sowie Geld sparen und sich in dieser eingesparten Zeit anderen Dingen widmen. Im Zeitalter des Internets erscheint es sinnvoll, dass eine Technologie in Form der AusweisApp angeboten wird und man auf die Verwendung des Internets zurückgreift.

Das Team der AusweisApp hat außerdem die Möglichkeit, die Anwendung stetig weiter zu entwickeln. Dank der finanziellen Mittel sind Studien wie zum Beispiel die des HPI finanzierbar, um Verbesserungspotential zu ermitteln. Hierzu zählen Änderungen der Sicherheitsbarrieren und eine Optimierung der Benutzerfreundlichkeit zur Steigerung der Akzeptanz der AusweisApp.

Threats

Gefahren der AusweisApp sind in den aufgezeigten Sicherheitslücken, wie dem verwendeten Computer, dem Kartenlesegerät und der AusweisApp selbst zu finden. Ein weiterer bedeutender Aspekt der Gefahren ist der Anwender. Er sollte hinreichend informiert sein über das Sicherheitsniveau seines Computers und den Einsatz und die Qualität des ausgewählten Kartenlesegerätes. Es sind jedoch auch banale Sicherheitsvorkehrungen zu beachten, wie beispielsweise der achtsame Umgang mit der PIN des Personalausweises.

Weitere mögliche Gefahren für die Akzeptanz sind die Nutzer selbst. Denn sie entscheiden, wie häufig die Online-Ausweisfunktion genutzt wird und somit auch, wie viele Institutionen aus Finanzen, Versicherungen und Behörden in den kommenden Jahren auf diese Technologie setzen werden. Außerdem gilt es an dieser Stelle Bezug auf die Mitarbeiter der Bürgerbüros zu nehmen, da sie in erster Linie Ansprechpartner für unsichere Bürger sind, wenn es darum geht, ob die Online-Ausweisfunktion des neuen Personalausweises freigeschaltet werden soll. Sie geben Empfehlungen und beantworten die ersten Fragen zur Dringlichkeit und Nützlichkeit dieses Dienstes. Natürlich ist es eine Gefahr für die Akzeptanz der AusweisApp, wenn Mitarbeiter den Nutzen der Online-Ausweisfunktion als negativ oder gering beschreiben.

4 Die „BürgerApp“

Das Open eCard-Team hat zwecks der neuen Einsatzmöglichkeiten der eID- und eSign-Funktion des neuen Personalausweises eine Initiative gestartet, um eine „leichtgewichtige, vertrauenswürdige und benutzerfreundliche Alternative“[125] zur AusweisApp bereitzustellen. Die Open-Source-Software soll, wie auch die AusweisApp, eine sichere Verbindung zwischen dem Kartenlesegerät des Benutzers, dessen Personalausweis und dem Diensteanbieter zur Datenübertragung herstellen.[126]

Dazu haben sich industrielle und akademische Experten aus Wirtschaft und Forschung zusammengeschlossen, um eine plattformunabhängige Programmierschnittstelle (engl. Application Programming Interface, API), basierend auf dem sogenannten eCard-API-Framwork [BSI-TR03112], zu programmieren, die verschiedenste Online-Anwendungen „für Zwecke der Authentisierung und Signatur leicht auf beliebige[n] Chipkarten“[127] ermöglichen soll und gleichzeitig die darin enthaltenen internationalen Standards umsetzt.[128] Die „BürgerApp“ soll nicht nur mit dem elektronischen Personalausweis funktionieren, sondern z.B. auch mit der Gesundheitskarte und ähnlichen Ausweisen, die über eine Chipkarte verfügen.[129]

Da das Ziel der Initiative ist, die BürgerApp als freie Software zur Verfügung zu stellen[130], besteht das Open eCard-Team aus einer offenen Gemeinschaft, an der „alle interessierten Bürgerinnen und Bürger sowie entsprechende Institutionen und Verbände“[131] mitwirken können, um die Anwendung kontinuierlich zu verbessern und benutzerfreundlicher zu machen. Durch die „Steigerung der Transparenz“[132] und die Möglichkeit der aktiven Bürgerbeteiligung erhofft sich das Open eCard-Team längerfristig eine Steigerung der Akzeptanz chipkartenbasierter Ausweise. Am 5. März 2013 veröffentlichte das Open eCard-Team den Source-Code zur ersten Version der BürgerApp.[133] Im Moment ist Version 1.0.4 verfügbar mit einer Größe von 4.6 Megabyte (MB).[134]

---

[125] prolicon GROUP (2013)
[126] Vgl. Bundesministerium des Innern (2013q)
[127] Dr. Wiesmaier, A. (2012), Seite 2
[128] Vgl. prolicon GROUP (2013)
[129] Vgl. Bürger-App.de (2013)
[130] Vgl. ebenda
[131] Dr. Wiesmaier, A. (2012), Seite 2
[132] Baader, H. (2013)
[133] Vgl. Bürger-App.de (2013)
[134] Vgl. CHIP Digital GmbH (2013)

4.1 Funktionalität

Wie eingangs angeführt, ist einer der wichtigen Punkte, der die BürgerApp von der AusweisApp abhebt, die Tatsache, dass die erstere auf dem eCard-API-Framework basiert und somit nicht nur den neuen Personalausweis sondern auch weitere Chipkarten unterstützt. Dem zugrunde liegt der nach CEN 15480 und ISO/IEC 24727 definierte CardInfo-Mechanismus[135], der im Wesentlichen die Online-Authentifizierung und elektronische Signatur mit folgenden Karten ermöglicht:[136]

- Die elektronische Gesundheitskarte (eGK)
- Der elektronische Personalausweis (ePA)
- Der elektronische Reisepass (ePass)
- Die elektronische Steuererklärung
- Der elektronische Einkommensnachweis (ELENA)

Der Ansatz des Open eCard Teams ist dabei, die entworfene App möglichst modular aufzubauen, sodass die Funktionalität jederzeit leicht geändert oder ergänzt werden kann. Dieser Erweiterungsmechanismus erlaubt es beispielsweise auch, die BürgerApp für weitere Authentisierungsmodule zugänglich zu machen. Während der neue Personalausweis nämlich das sogenannte Password Authenticated Connection Establishment (PACE)- und Extended Access Control (EAC) Protokoll verwendet, werden bei vielen anderen, in Europa ausgegebenen Signatur- und Ausweiskarten GenericCryptography- und PIN Compare Protokolle eingesetzt[137]. Dank des eCard-API-Frameworks, das eine einfache und homogene Schnittstelle bereitstellt, kann die Kommunikation zwischen der Anwendung und den verschiedenen Chipkarten vereinheitlicht werden[138].

Gerade die elektronische Gesundheitskarte findet bereits Anwendung und dürfte zukünftig von großem Interesse sein. Da der Fokus dieses Projekts jedoch auf dem elektronischen Personalausweis liegt, wird die BürgerApp in den folgenden Abschnitten lediglich in Verbindung mit diesem untersucht.

---

[135] Vgl. Horsch, M. et alii (2013), S. 508
[136] Vgl. Bundesamt für Sicherheit in der Informationstechnik (o.J. g)
[137] Vgl. Horsch, M. et alii (2013), S. 508
[138] Vgl. Bundesamt für Sicherheit in der Informationstechnik (o.J. h)

4.2 Ressourcenanforderungen und Kompatibilität

Eine besondere Problematik entsteht dadurch, dass die BürgerApp auf verschieden Betriebssystemen lauffähig sein soll. Wie eben erwähnt, fördern der „hochgradig modulare Ansatz“ der Architektur und die java-basierte Realisierung der BürgerApp eine leichte Erweiterbarkeit und den Einsatz auf unterschiedlichen Plattformen.[139]

Um den elektronischen Personalausweis für die Authentisierung im Internet zu nutzen, muss die BürgerApp als „eID-Client“ aus dem Browser heraus aktiviert werden, um eine Verbindung zum „eID-Server“ aufzubauen, mit dem die eigentliche Authentisierung (z.B. mit dem EAC Protokoll) durchgeführt wird.[140]

Nutzerinnen und Nutzer müssen dazu einen Rich Client als „dauerhaft[e] (…) Anwendung für stationäre[..] Betriebssysteme“ als Programm, die BürgerApp, auf ihrem Computer installieren.[141] Der Rich Client ist eine Java SE[142] Applikation. Das bedeutet, dass als Voraussetzung Java Runtime 1.6 oder höher auf dem Client-Rechner installiert sein muss, um die BürgerApp installieren zu können.[143,144] Die Java Laufzeitumgebung kann kostenlos auf der Homepage von Oracle heruntergeladen werden.[145] Damit ist die BürgerApp als plattformunabhängige Java-Applikation auf nahezu allen Betriebssystemen lauffähig, wie Windows XP, Windows Vista, Windows 7, Windows 8, Linux und Mac OS.

Die BürgerApp wird dabei üblicherweise auf dem Rechner in einer betriebssystemspezifischen Weise installiert und kann anschließend vom Benutzer aus aufgerufen werden.[146]

Über den Browser kann ein Setup-Assistent für die BürgerApp aufgerufen werden, den das Open eCard Team für die Betriebssysteme unter den Downloads auf seiner Seite bereitstellt: https://www.openecard.org/download/pc.[147,148] Nach erfolgreicher Installation wird der Set-Up-Assistent beendet und die BürgerApp kann als Desktop Applikation aufgerufen werden.

---

[139] Vgl. Dr. Wiesmaier, A. (2012), Seite 4
[140] Vgl. Open eCard Team (2013a)
[141] Vgl. Dr. Wiesmaier, A. (2012), Seite 7
[142] Java Platform Standard Edition
[143] Vgl. CHIP Digital GmbH (2013)
[144] Vgl. Redmine (2013a)
[145] Download verfügbar unter: http://www.oracle.com/technetwork/java/javase/downloads/index.html
[146] Vgl. Redmine (2013a)
[147] Vgl. Redmine (2013b)
[148] Vgl. Redmine (2013a)

Abb. 4: Setup-Assistent der BürgerApp[149]

Bei der Benutzung wird das in Java implementierte Programm vom Benutzer über den Webbrowser aus per localhost-Link oder einem eingebetteten Object-Tag aktiviert, z.B. bei der Nutzung eines Online-Dienstes.[150] Damit die BürgerApp von browser-gestützten Webanwendungen genutzt werden kann und nicht nur in Verbindung mit festinstallierten Anwendungen, wird in der Architektur die Komponente eines client-seitigen „spezifizierte[n], http-basierte[n] eID-Aktivierungsmechanismus“[151] umgesetzt. Nutzerinnen und Nutzer können mit der BürgerApp weiterhin ihren gewohnten aktuellen Browser wie Internet Explorer, Opera, Chrome oder Firefox betreiben und auf alle Features zugreifen. Längerfristig ist die tiefere Integration der BürgerApp in populäre Browser geplant.[152] Nun ist zur Verwendung der BürgerApp keine proprietäre Software mehr notwendig.[153]

Die BürgerApp unterstützt entweder SOCKS oder HTTP Proxies, die folgende Eigenschaften besitzen:

SOCKS:
proxy.socks.host = localhost -- Hostname or IP address of the server where the proxy server is running on.
proxy.socks.port = 8080 -- Port on the proxy host where the proxy service is listening on.

[149] Hühnlein, D. (2012)
[150] Vgl. prolicon GROUP (2013)
[151] Dr. Wiesmaier, A. (2012), Seite 6
[152] Vgl. Dr. Wiesmaier, A. (2012), Seite 6
[153] Vgl. Bürger-App.de (2013)

HTTP(S):
proxy.http.scheme = http -- specifies the protocol scheme of the proxy (http or https)
proxy.http.host = localhost -- Hostname or IP address of the server where the proxy server is running on.
proxy.http.port = 8123 -- Port on the proxy host where the proxy service is listening on.
proxy.http.user = foo -- User name for basic authentication (optional).
proxy.http.pass = bar -- Password for basic authentication (optional).
proxy.http.validate_tls = false -- specifies that the certificate of the proxy service is not validated against the java key store (optional)[154]

Danach muss der Personalausweis auf das mit dem Rechner verbundene Kartenlesegerät gelegt werden, damit der Online-Dienstleister auf die Berechtigung der Datenabfrage überprüft werden kann. Mit der Eingabe des PINs stimmt der Benutzer der Übermittlung der Daten zu. Für die BürgerApp wird lediglich der Basiskartenleser benötigt, bei dem die PIN-Eingabe über die Tastutur des angeschlossenen Rechners erfolgt.

Auch für das mobile Betriebssystem Android ist eine Authentisierung mit dem neuen Personalausweis möglich. Hierfür werden Smartphones oder Tablets mit Android Version 4.1 oder höher benötigt, sowie ein Universal Serial Bus (USB)-Anschluss.[155] Zurzeit funktioniert die BürgerApp lediglich auf dem Galaxy Nexus S und Asus Transformer TF300T.[156] Benötigt werden wieder ein Kartenleser (z.B. Basiskartenleser), ein USB-Kabel zur Verbindung mit dem Kartenleser oder ein Keydock mit USB-Verbindung, sowie der Personalausweis. Die Bürger-App kann über den Aufruf eines Links im Browser auf das Android-Gerät installiert werden.[157] Dazu muss der Link zur BürgerApp APK[158] angeklickt werden und die Installation der heruntergeladenen APK akzeptiert werden.[159]

4.3 Sicherheitsaspekte

Hintergrund der Entwicklung einer Online-Authentifizierung ist vor allem die Suche nach neuen Möglichkeiten, sich sicher im Internet auszuweisen. Das derzeit weitverbreitetste Verfahren ist der Einsatz von Passwörtern, die im Allgemeinen aber eher als unsicher eingeschätzt werden, da sie den Identitätsdiebstahl und –missbrauch nur bedingt verhindern können. Dies resultiert daraus, dass Endanwender häufig das gleiche Passwort für verschiedene Anwendungen nutzen, während das Erspähen oder Erraten von Passwörtern beziehungs-

[154] Redmine (2013a)
[155] Vgl. Open eCard Team (2013b)
[156] Vgl. Petrautzki, D. (2012)
[157] Vgl. Petrautzki, D. (2012)
[158] Android application package file
[159] Vgl. Petrautzki, D. (2012)

weise auch Ermitteln durch Schadsoftware gleichzeitig verhältnismäßig leicht ist[160]. Nichtsdestotrotz konnten sich in der Internetwelt bisher keine wirklichen Alternativen zu Passwörtern durchsetzen, da es diesen häufig an Benutzerfreundlichkeit oder Handhabbarkeit mangelt. „Außerdem verlangen viele Alternativen spezielle Anpassungen auf Client- und Server-Seite und sind zudem kostspielig.“[161] Durch die Einführung des neuen Personalausweises wird nun ein Weg geschaffen, der eine „sichere Zwei-Faktor-Authentisierung im Internet“[162] ermöglicht. Für die Online-Ausweisfunktion benötigt der Nutzer nunmehr nicht nur eine PIN sondern auch den Ausweis an sich. Durch den Verlust beziehungsweise Diebstahl der PIN oder des Dokumentes alleine wird folglich noch kein Identitätsdiebstahl möglich[163].

Wie bereits im Kapitel zur AusweisApp ausgeführt, ergeben sich aus dem Einsatz des Personalausweises als Identifizierungsdokument im Internet gleichzeitig auch einige allgemeine Sicherheitsprobleme, die sich in die bereits spezifizierten vier Bereiche einteilen lassen. Um Wiederholungen aus dem vorhergegangenen Kapitel zu vermeiden, werden im Folgenden die allgemein bestehenden Probleme lediglich noch einmal näher durch Beispiele beleuchtet, bevor auf die BürgerApp selbst eingegangen werden soll.

4.3.1 Allgemeine Sicherheitslücken

Trotz umfangreicher technischer Maßnahmen, die einen möglichst hohen Datenschutz sicherstellen sollen[164], kann es auch beim Einsatz des neuen Personalausweises zu Identitätsmissbrauch kommen. In Abhängigkeit des benutzten Kartenlesegerätes, kann es zum Mitlesen der PIN kommen. Wird beispielsweise ein Kartenlesegerät der Klasse 1 ohne eigene Tastatur verwendet und die PIN somit am Computer eingegeben, können spezielle Malwareprogramme diese erfassen[165]. Befindet sich der Personalausweis gleichzeitig in Reichweite des Kartenlesegerätes, kann das Protokoll auch von jemand Fremdes erfolgreich durchgeführt werden[166]. Dem kann allerdings durch die Eingabe der PIN am Kartenlesegerät selbst vorgebeugt werden[167]. Zudem kann es bei der eigentlichen Authentisierung zu einem Missbrauch kommen. Für die Ausweisfunktion ist eine Verbindung des Bürgerclients mit dem eID-Server nötig, diese „Sitzung“, die zwischen dem normalen Browser und der Webanwendung aufgebaut wird, kann bei einer unsicheren Verbindung auf die Sitzung des Angreifers

[160] Vgl. Schröder, M. / Morgner, F. (2013), S. 530
[161] Ebenda, S. 530
[162] Ebenda, S. 530
[163] Vgl. Schröder, M. / Morgner, F. (2013), S. 530
[164] Vgl. Borges, G. et alii (2011), S. 163
[165] Vgl. ebenda, S. 171
[166] Vgl. ebenda, S. 166
[167] Vgl. ebenda, S. 171

„umgeleitet“ werden[168]. Diese Schwachstelle kann auch ganz gezielt ausgenutzt werden, um eine anonyme Altersverifikation im Internet zu umgehen. Wenn auch für den kommerziellen Missbrauch uninteressant, könnte ein Minderjähriger bei Kooperation mit einem volljährigen Personalausweisbesitzers auf Internetseiten mit Altersbeschränkung zugreifen. Verbindet sich der Volljährige dauerhaft mit einer Serverapplikation, kann sich der Minderjährige durch ein Browser-Plug-in ebenfalls mit diesem Server verbinden und seine vermeintliche Volljährigkeit gegenüber einer Webapplikation verifizieren[169].

Es bestehen darüber hinaus weitere, ähnliche Szenarien wie beispielsweise beim Man-in-the-Middle-Angriff, bei dem ein Dritter einerseits eine Verbindung mit dem eID Server und gleichzeitig eine SSL (Secure Socket Layer) Verbindung mit dem Opfer aufbaut und so auf dessen vertrauliche Daten zugreifen kann[170]. Diese zuletzt geschilderten Probleme sind aber nicht spezifisch für die Authentifizierung mit dem neuen Personalausweis sondern gelten für die meisten Online-Ausweisverfahren[171].

4.3.2 Sicherheitsaspekte der BürgerApp

Für das Team der Open eCard ist Sicherheit ein zentrales Qualitätsmerkmal bei der Entwicklung der BürgerApp. Das nachfolgende Diagramm zeigt, dass der Aspekte der Sicherheit dabei dem Bereich der Funktionalität der BürgerApp zugeordnet wird und neben der bereits angesprochenen Benutzerfreundlichkeit als ein „extrem wichtiges“ Merkmal eingestuft wird.

Abb. 5: Qualitätskriterien für die Open eCard App[172]

---

[168] Vgl. Borges, G. et alii (2011), S. 161
[169] Vgl. ebenda, S. 173
[170] Vgl. ebenda, S. 173 f.
[171] Vgl. ebenda, S. 174
[172] Entnommen aus: Hühnlein, D. (2013a), Folie 12

Betrachtet man die derzeitige Version der Open eCard App, so ist in Bezug auf die Sicherheit ihre Open Source Verfügbarkeit hervorzuheben. Einerseits wird die offene Zugänglichkeit des Quellcodes auf Github lobend hervor gehoben, da auf diese Art und Weise jeder die Möglichkeit hat, die App auf eventuelle Sicherheitslücken zu prüfen und sie somit gestärkt wird. Unabhängige Experten können den Quellcode überprüfen, was die Transparenz und somit auch das Vertrauen in die Anwendung erhöht. Neben der gesteigerten Sicherheitsbasis und der verbesserten Modifizierbarkeit fördern Open-Source Projekte zudem „Anreiz und Impulse für Innovation und Forschung“[173].

Gleichzeitig birgt die Tatsache aber natürlich auch die Gefahr, dass ein Angreifer eine identische Applikation nachbauen kann, um auf diese Art und Weise Nutzer der Online-Ausweisfunktion durch eine überzeugend echt wirkende Anwendung zu täuschen und so die persönlichen Daten auszulesen.

Ein weiterer Aspekt, der die Sicherheit der Open eCard App steigert, ist, dass die Anwendung plattformunabhängig läuft und somit auch die neuesten Browser mit den höchsten Sicherheitsstandards unterstützt. So profitiert der Nutzer von der ständigen Weiterentwicklung der Internetzugänge[174]. Außerdem unterstützt die Open eCard App die CORS-basierte Erkennung einer App[175]. Dieser Mechanismus des „Cross-Origin Resource Sharing“ erlaubt Webbrowsern oder auch anderen Webclients Cross-Origin Requests, die normalerweise aufgrund der Same-Origin-Policy (SOP) untersagt wären. Diese Einschränkungen können jedoch vom jeweils anfragenden Server durch bestimmte HTTP Header für bestimmte Clients aufgehoben werden[176]. Neben der Sicherheit steigert dieser Ansatz gleichzeitig auch die Flexibilität der Anwendung[177].

Zuletzt soll an dieser Stelle noch darauf eingegangen werden, dass das Team der Open eCard App bestrebt ist, sowohl etablierte Authentisierungsprotokolle wie das TLS-Protokoll als auch attribut-basierte, datenschutzfreundliche Credentials wie das vom Personalausweis verwendete EAC-Protokoll zu unterstützen. Dieses alternative Verfahren erlaubt sowohl eine starke Authentisierung als auch einen sparsamen Umgang mit den vertraulichen Daten des Nutzers und wird daher als datenschutzfreundlicher angesehen[178].

---

[173] Wiesmaier, A. (2013), S. 2
[174] Vgl. Kühne, A. (2013)
[175] Vgl. Hühnlein, D. (2013a), Folie 27
[176] Vgl. Mozilla Developer Network (2013)
[177] Vgl. Kühne, A. (2013)
[178] Horsch, M. et alii (2013), S. 510

4.4 Benutzerfreundlichkeit

Vorwegnehmend kann gesagt werden, dass die Benutzerfreundlichkeit der BürgerApp sehr hoch eingeschätzt wird. Dies resultiert aus dem Ansatz als Open Source Projektes, da so „nicht nur Informatiker und Sicherheitsexperten die App aus ihrer technischen Sichtweise testen“[179]. Durch den offenen Dialog mit allen interessierten Bürgern erhofft sich das Open eCard Team eine kontinuierliche Verbesserung der Benutzerfreundlichkeit. Ideen und Vorschläge können dabei auf der Projektseite der Open eCard veröffentlicht werden, um darüber zu diskutieren und gegebenenfalls die Umsetzung anzustoßen[180]. Die Implementierung einer neuen graphischen Benutzeroberfläche (GUI) beziehungsweise die Verbesserung einer bestehenden Version wird dabei durch die Abstraktion der Schnittstelle erleichtert. Auf diese Art und Weise kann die GUI jederzeit durch eine andere Version ersetzt werden oder auch Plattform-spezifisch implementiert werden, ohne dabei für andere Module Änderungen vornehmen zu müssen[181]. Das Team um die BürgerApp hat sich dabei selbst zum Ziel gesetzt, die Oberfläche möglichst benutzerfreundlich und zugänglich zu gestalten[182]. So wurde die erste Version der Benutzeroberfläche direkt nach Start des Projektes überarbeitet, um ein klares Layout umzusetzen. Die beiden Alternativen sehen dabei folgendermaßen aus:

Abb. 6: Gegenüberstellung des alten und neuen Layouts der BürgerApp

Am ursprünglichen Layout, wie auf der linken Seite gezeigt, wurde bemängelt, dass weder gültigen Einzüge vorhanden seien (im Bild in orange markiert) noch eine klare Struktur erkennbar sei[183]. Dadurch würde die gesamt App für den Benutzer „unaufgeräumt“ wirken[184]

179 Bürger-App (2013)
180 Vgl. Hühnlein, D. (2013b)
181 Vgl. Wiesmaier, A. (2013), S. 5
182 Vgl. Hühnlein, D. et alii (2013), S. 100
183 Vgl. Schumacher, F. (2012)

Der neue Entwurf hingegen mache die Grundstruktur schnell begreifbar, da die Einzüge auf lediglich vier begrenzt würden (orange hervorgehoben) und ein Strich (im Bild grün eingerahmt) ein eindeutiges Raster in das Layout brächte[185]. Nach Eingang des Vorschlages zur Überarbeitung des Layouts, wurde die entsprechende Implementierung innerhalb von nicht einmal einem Monat in den Projektrahmen mit aufgenommen und einen weiteren Monat später bereits realisiert[186]. Dies zeigt, welche Mitbestimmungsmöglichkeiten die Bürger bei der Gestaltung der App besitzen. Gleichzeitig verdeutlichen die Bilder den simplen Aufbau der App und die daraus resultierende Benutzerfreundlichkeit. In drei einfachen Schritten wird der Anwender durch die Applikation geführt – nach einer Übersicht zu dem Anbieter des Online-Ausweisverfahrens, wird der Nutzer über den Umfang der angefragten Daten informiert, bevor er den Vorgang schließlich mit der PIN Eingabe abschließt. Die übersichtlich gestaltete Anwendung führt logisch durch die Online-Authentifizierung und garantiert somit eine intuitive BürgerApp.

Auch die Plattform-Unabhängigkeit trägt zur Benutzerfreundlichkeit bei, da der Endanwender so das Betriebssystem sowie den Browser seiner Wahl zur Ausführung der Online-Authentifizierung nutzen kann und nicht gezwungen ist, auf unterstützte Alternativen umzusteigen[187].

Alles in allem handelt es sich durch das Mitwirken vieler Interessensgruppen bei der BürgerApp um eine sehr benutzerfreundliche Anwendung.

4.5 Administration

Unternehmen, die auf ihren Online-Portalen die neue Ausweisfunktion des Personalausweises anbieten wollen, müssen ihren Kunden, die den Service in Anspruch nehmen möchten, mit einer gewissen Supportfunktion unterstützen. Nutzerinnen und Nutzer, die die BürgerApp auf ihren Rechnern installiert haben oder interessiert sind, via dieser den Datenverkehr zwischen Dienstanbieter und Kartenlesegerät regeln, erwarten spezifische Serviceleistungen bei Fragen und Problemen zur BürgerApp. Die Administration der BürgerApp gestaltet sich allerdings als relativ schwer, da die Software nicht direkt in Verbindung mit dem Online-Dienstanbieter steht. Die Wahl der Software sowie dessen Installation erfolgen vollständig über den Benutzer.

---

[184] Schumacher, F. (2012)
[185] Vgl. ebenda (2012), Folie 3
[186] Vgl. Wieland, T. (2013)
[187] Vgl. Open eCard Team (2013c)

Online-Dienstanbieter können allerdings während dem gesamten Prozess ihre Kunden von der Auswahl der Verbindungs-Software bis hin zu Fehlermeldungen begleiten, indem ausreichend Informationen vermittelt werden. Bei Empfehlung der BürgerApp sollte der Online-Dienstanbieter das Open eCard-Projekt und die Idee dahinter vorstellen. Eine Auflistung der Vorteile der BürgerApp gegenüber anderen Anbietern, die benötigen technischen Voraussetzungen und ein User Guide zur Installation und Benutzung der BürgerApp sowie eine FAQ-Liste helfen Nutzern und Interessenten, sich mit der BürgerApp schneller vertraut zu machen. Dies kann über Verlinkungen zur Open eCard- und BürgerApp-Homepage oder durch die direkte Einbettung einer Informationsseite in die unternehmenseigene Homepage des Online-Dienstanbieters erfolgen.

Eine Supportfunktion bei Fehlermeldungen zur BürgerApp selbst kann nur schwer vom Online-Dienstanbieter behandelt werden, da die Verbindungssoftware in keinen direkten Kontakt mit den Unternehmen hat. Auch eine Weiterleitung an das Open eCard-Team selbst erweist sich als schwierig, da dieses aus einer offenen Gemeinschaft besteht. Da sich die BürgerApp derzeit noch in der Entwicklung befindet und keine endgültige Version vorliegt, ist noch keine spezifische Support-Abteilung vorhanden. Das Open eCard-Team setzt momentan viel mehr darauf, dass Anmerkungen und Vorschläge über die Homepage eingereicht werden, sodass diese in die finale Version eingebaut werden können.

Um dennoch die Frage der Administration persönlicher zu beantworten, können Online-Dienstanbieter die Projektmanager der BürgerApp kontaktierten. Diese sind auf der Projektmanagement-Webseite (http://dev.openecard.org/projects/open-ecard) der BürgerApp aufgelistet, die vom Projektmanagement-Tool redmine betrieben wird. Hier sind auch die Projektfortschritte des Open eCard-Teams öffnetlich zugänglich und können von jedermann kommentiert werden.

4.6 SWOT Analyse des Programms

Interne Analyse	**Strenghts** – Leichtgewichtige Implementierung – Plattformunabhängige Software für unterschiedliche Betriebssysteme – Vom Browser unabhängige Anwendung – Unterstützung des mobilen Betriebssystems Android – Keine proprietäre Software notwendig – Vermeidung von mangelhafter Systemintegration und Sicherheitsrisiken eines Java-Plugins im Browser – Authentisierung und Signatur mit beliebigen Chipkarten – Intuitive Bedienung	**Weaknesses** – BürgerApp befindet sich noch Entwicklungsstadium – Schlechte Administrationsmöglichkeiten durch fehlendes Organisationsteam (non-profit) – Keine weiteren Erklärungen, Anleitungen, User Guides vorhanden
Externe Analyse	**Opportunities** – Steigerung der Transparenz und des Vertrauens in die Sicherheitstechnologie durch Open-Source-Software – Aktive Bürgerbeteiligung (Bewertungen, Tests, Vorschläge, Kritik) → Steigerung der Akzeptanz → Kontinuierliche Verbesserung der Benutzerfreundlichkeit	**Threats** – Missbrauch des offenen Quellcodes, um eine täuschend echte BürgerApp zu konstruieren – Allgemein wenige Anbieter für Online-Dienste mit dem neuen Personalausweis

Strenghts

Die Stärken der Anwendung liegen klar in ihrem modularen Aufbau, leichtgewichtigen und plattformunabhängigen Implementierung sowie den wenigen Voraussetzungen, die für ihren Gebrauch nötig sind. So kann die Anwendung mit allen gängigen Betriebssystemen und Browsern verwendet werden, ohne dass weiter proprietäre Software nötig wäre. Außerdem wird bereits an der Unterstützung des mobilen Betriebssystem Androids gearbeitet und der Aufbau der App so gehalten, dass sie auch mit anderen Chipkarten verwendet werden kann.

Weaknesses

Die BürgerApp befindet sich noch in einem Entwicklungsstadium, da sie durch keine offizielle Instanz finanziert wird, mangelt es gegebenenfalls an Geldern und Personal für die weitere Unterstützung und den Support des Endanwenders. Die bisherige Dokumentation ist eher dürftig, da keine FAQ-Listen oder User Guides für den Nutzer vorliegen.

Opportunities

Da der Quellcode des Programms offen zugänglich ist, können unabhängige Experten diesen auf Sicherheitslücken prüfen. Gleichzeitig steigert dies die Transparenz und damit das Vertrauen des Endanwenders in die Anwendung. Da jeder Bürger dazu eingeladen ist, sich an der Entwicklung der Applikation zu beteiligen, kann die Vertretung der verschiedenen Interessensgruppen zu der Benutzerfreundlichkeit beitragen und auch die allgemeine Akzeptanz der Online-Ausweisfunktion steigern.

Threats

Die Verfügbarkeit des Quellcodes als Open Source bildet auch ein mögliches Risiko, da Angreifer den Code dazu nutzen können, eine vergleichbare Anwendung zu bauen, um den Anwender zu täuschen und so seine Daten zu ermitteln.

Außerdem mangelt es derzeit insgesamt noch an der Akzeptanz des neuen Personalausweises, wobei die verschiedenen verfügbaren Programme dazu führen können, dass das Vertrauen weiter sinkt.

5 Bewertung der Ergebnisse

Dieses Kapitel soll dazu dienen, das Potential des neuen Personalausweises als Identifikationsmittel bei einem Online-Portal zu bewerten. Zu diesem Zweck werden die Ergebnisse aus den vorhergegangenen SWOT Analysen der beiden Programme zunächst noch einmal gegenübergestellt. Im Anschluss daran, werden noch mögliche Alternativen aufgezeigt, die neben dem Personalausweis verwendet werden könnten, um den Zugang zu dem Portal zu autorisieren. Abschließend bildet die Empfehlung für das Unternehmen das Fazit der Arbeit.

5.1 Vergleich der beiden Programme

Wie aus den SWOT Analysen der beiden Programme AusweisApp und BürgerApp hervorgeht, weisen beide Vor- und Nachteile auf. Im Folgenden sollen die Anwendungen anhand der einzelnen identifizierten Aspekte noch einmal im direkten Vergleich betrachtet werden.

Ressourcenanforderungen und Komptabilität

Was die Komptabilität der beiden Anwendungen angeht, fällt auf, dass die BürgerApp im Gegensatz zur AusweisApp weitaus mehr Betriebssysteme und Browser unterstützt. Während die AusweisApp zwar mit allen gängigen Windows-Versionen genutzt werden kann, ist die Anpassung an Mac OS bisher nur teilweise realisiert worden und auch Ubuntu-Nutzer müssen gegebenenfalls auf die 32-bit Variante umsteigen.

Bei der BürgerApp benötigt der Nutzer als einzige Voraussetzung Java Runtime 1.6 oder höher, damit er die Anwendung auf seinem Computer installieren kann. Abgesehen von dieser kostenlos erhältlichen Laufzeitumgebung ist die BürgerApp plattformunabhängig und unterstützt somit alle Betriebssysteme und Browser.

Für beide Programme wird gleichermaßen ein Kartenlesegerät benötigt, das je nach Funktionalität zwischen 20€ und 160€ kostet.

Sicherheitsaspekte

Der Aspekt der Sicherheit steht für das Unternehmen im Vordergrund und wurde daher umfassend beleuchtet. Es zeigt sich, dass für beide Programme gewisse Sicherheitslücken bestehen, die eine Gefahr für den Nutzer darstellen. Diese allgemeinen Aspekte ergeben sich aus dem Computer, der für die Online-Authentifizierung genutzt wird, sowie aus dem Kartenlesegerät und dem Nutzer selbst.

Unabhängig von der verwendeten Anwendung, besteht das Risiko, das der Schutz des Anwender-PCs aus Unkenntnis oder Nachlässigkeit unzureichend ist und somit einen externen Zugriff auf die Daten erlaubt. Durch veralteten Virenschutz oder Firewalls, sind Szenarien

denkbar, in denen Malware auf den Computer eingeschleust wird, um die gespeicherten Daten aufzurufen. Auch ein Man-in-the-Middle-Angriff oder die gezielte Umgehung von Altersverifikationen ist in beiden Fällen möglich und macht den Gebrauch der entsprechenden Funktion unsicher. Wie bereits angesprochen variieren die Kosten und Funktionalitäten der Kartenlesegeräte und damit einher geht auch ein unterschiedliches Level an Sicherheit. So wird von den günstigen Basis-Kartenlesegeräten, die weder Display noch Tastatur aufweisen, abgeraten, da die Eingabe der PIN am Computer ein Mitlesen der Nummer durch Malware möglich macht. Zwar ist für den Missbrauch der Online-Authentifizierung neben der PIN auch der Personalausweis selber nötig, doch befindet sich dieser noch in Reichweite des Kartenlesegerätes, kann das Protokoll auch von jemand Fremdes durchgeführt werden.

Daraus ergibt sich auch der dritte Risikofaktor, der beide Applikationen betrifft: der Nutzer selbst. Bei fahrlässigem Umgang mit der PIN oder dem Ausweisdokument, können Externe gegebenenfalls auf die Daten des Besitzers zugreifen. Daher sollte der Anwender nur dann von der Online-Ausweisfunktion Gebrauch machen, wenn er sich der nötigen Sicherheitsprogramme auf seinem Computer bewusst ist und seine Daten vertraulich behandelt.

Neben diesen allgemeinen Punkten gibt es auch unterschiedliche weitere Angriffspunkte bei Nutzung der beiden Programme. Während das Open eCard Team den Quellcode der Bürger-App öffentlich zugänglich gemacht hat, ist der Source Code der AusweisApp nicht einsehbar. Nachdem die AusweisApp bereits erfolgreich gehackt wurde, wird aus diesem Grund die BürgerApp lobend hervorgehoben, da unabhängige Experten Lücken im Code aufdecken und melden können. Andererseits entsteht durch den offenen Quellcode auch die Gefahr, dass Angreifer eine täuschend echte Nachbildung der BürgerApp gestalten, um so die Daten der Anwender zu erspähen.

In Bezug auf die BürgerApp ist außerdem hervorzuheben, dass ihre Plattformunabhängig die Nutzung der neuesten Browsern erlaubt, die mitunter einen höheren Sicherheitsstandard aufweisen, als veraltete Versionen. Die AusweisApp auf der anderen Seite erlaubt es dem Anwender nicht, bei der Online-Authentifizierung Cookies zu deaktivieren, was einen potentiellen Angriffspunkt zum Auslesen der Daten bietet.

Ein entscheidender Faktor der die beiden Anwendungen auf die gleiche Art und Weise betrifft, ist die fehlende Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik. Während die AusweisApp seit 2012 auf das entsprechende Zertifikat wartet, das aufgrund von noch nicht abgeschlossenen „Test- und Analysemaßnahmen zur Qualitätssicherung und Sicherheitsbewertung“[188] bisher nicht vergeben wurde, gibt es über die BürgerApp zu diesem Thema keine weiteren Informationen. Laut Bundesrechnungshof kann der

[188] Heise Online (2013)

Mangel einer Zertifizierung zu „Haftungsrisiken bei den Ausweisinhabern führen“[189] und sei daher inakzeptabel[190].

Es zeigt sich, dass beide Programme ähnliche, mitunter schwerwiegende, Sicherheitslücken aufweisen, der größte Unterschied liegt in der Verfügbarkeit des Quellcodes sowie der Browser-Unterstützung. Hier scheinen die Vorteile der BürgerApp zu überwiegen, da der Code sowohl durch unabhängige Experten geprüft wurde und die Unterstützung der neuesten Browserversionen die höchsten Sicherheitsstandards garantiert.

Benutzerfreundlichkeit

Was die Benutzerfreundlichkeit angeht, ist vorwegnehmend anzumerken, dass durch die Studie des Hasso-Plattner-Instituts weitaus umfassendere Ergebnisse für die AusweisApp vorliegen als für die BürgerApp. Die Studie hat ergeben, dass die Benutzerfreundlichkeit der AusweisApp durch allgemeine Unwissenheit über die Online-Authentifizierung, begriffliche Unverständlichkeiten innerhalb der Applikation sowie unzureichende Erläuterungen während des Prozesses bei allen Zielgruppen Kritik erfahren musste.

Für die BürgerApp gibt es keine vergleichbare Analyse, allgemein wird ihre Benutzerfreundlichkeit allerdings als vergleichsweise hoch eingeschätzt, da die Mitarbeit unterschiedlicher Interessensgruppen dazu führt, dass diese anwenderfreundlich und intuitiv gestaltet und weiterentwickelt wird. Auch an dieser Stelle muss zudem die Plattformunabhängigkeit dieser Applikation genannt werden, da der Anwender so nicht gezwungen wird, sich an ein alternatives System zu gewöhnen.

Administration

Da die AusweisApp durch den Bund finanziert und unterstütz wird, scheint die Applikation in Bezug auf die Administration Vorteile gegenüber der BürgerApp aufzuweisen. Die BürgerApp befindet sich noch in einer beta-Version, zwar ist sie bereits offiziell verfügbar und nutzbar, doch befindet sie sich noch in der Weiterentwicklung. Aus der offenen Teamstruktur resultiert, dass es keine festen Ansprechpartner bei Problemen oder Fragen gibt; Wünsche und Anregungen können zwar auf der Internetseite des Open eCard Teams geäußert werden, doch gibt es keinen direkten Kontakt zu dem Anbieter oder eine Supportfunktion beziehungsweise –hotline.

Die AusweisApp unterstützt den Anwender durch eine Liste an häufigen Fragen mit den zugehörigen Antworten, die auf der Website der Applikation zu finden ist. Diese FAQ-Auflistung behandelt neben allgemeinen Aspekten die Ressourcenanforderung und Komptabilität, Si-

---

[189] Heise Online (2013)
[190] Vgl. ebenda

cherheit, Online-Ausweisfunktion sowie bekannte Probleme und Fehlermeldungen und stellt somit eine hilfreiche Unterstützung für den Nutzer dar. Obwohl auch hier keine Hotline genannt wird, steht dem Anwender ein Webformular als Supportfunktion zur Verfügung, durch das er Probleme melden kann. Alternativ kann sich der Nutzer der AusweisApp auch direkt an das BSI wenden, um seine Anregungen zu äußern.

5.2 Mögliche Alternativen

Nachdem die Möglichkeit, den Kundenbereich einer Website mithilfe des neuen Personalausweises zu schützen nun sowohl erläutert als auch bewertet wurde, sollen im Folgenden einige Alternativen angesprochen werden, wie ein Online-Kundenbereich ebenfalls geschützt werden könnte.

Passwort

Die naheliegende und einfachste Möglichkeit, einen Online-Kundenbereich zu schützen, ist mithilfe eines individuellen Benutzernamens und Passwort. Diese Möglichkeit bietet den Vorteil, dass neue Accounts sehr einfach zu erstellen sind, Nutzern im Falle eines vergessenen Passworts schnell geholfen werden kann und diese Möglichkeit auch für den Anwender am einfachsten zu nutzen ist und nicht vieler Erklärungen bedarf.

Die Sicherheit kann durch spezielle Anforderungen an das Passwort (Länge, Einsatz großer und kleiner Buchstaben, sowie von Zahlen) erhöht werden und zusätzlich durch eine verschlüsselte Übertragung der Benutzernamen und Passwörter zum Server verstärkt werden.

Der Schutz von Websites oder spezieller Bereiche mittels Passwort ist die wohl gängigste Sicherungs-Technik, was sich beispielsweise dadurch belegen lässt, dass ein Großteil der Banken und Versicherung diese Technik nutzen.

Dennoch besteht hier ein Restrisiko, das definitiv zu beachten ist. So bietet diese Technik keinen hundertprozentigen Schutz, was durch teilweise großflächige Passwort-Hacks auch bei renommierten Unternehmen gezeigt wurde. Immer wieder wird über illegale Vorgänge berichtet, beispielsweise bei Apple[191], Sony[192] oder Microsoft[193].

[191] Vgl. Giga (2012)
[192] Vgl. Computer Bild (2013)
[193] Vgl. t3n (2012)

TAN-Verfahren

Neben einer Zugangssicherung per Passwort wäre zusätzlich eine Zugangssicherung per TAN-Verfahren denkbar. Eine Transaktionsnummer (TAN) kann als einmaliges Passwort betrachtet werden.

In seiner ursprünglichen Form wird bei dieser Identifizierungs-Technik dem Kunden zunächst eine Liste mit einer bestimmten Anzahl durchnummerierter Passwörter zugesandt. Sobald sich der Kunde nun online identifizieren will, wird von der Website neben Benutzername und Passwort zusätzlich eine der TAN-Nummern aus der Liste abgefragt. Nach der Benutzung der TAN-Nummer wird diese aus der Liste gestrichen.

Das ursprüngliche TAN-Verfahren wurde bereits mehrfach weiterentwickelt und so ist neben dem Einsatz von Listen mittlerweile auch die Möglichkeit gegeben, die TAN-Nummern per SMS oder TAN-Generator zu empfangen. Dies sichert das TAN-Verfahren nochmals zusätzlich gegen Fishing-Angriffe ab.[194]

Haupteinsatzbereich des TAN-Verfahrens ist momentan das Online-Banking, wo die Kunden jede Überweisung durch die Eingabe einer TAN-Nummer bestätigen müssen. Alternativ ist aber auch der Einsatz des TAN-Verfahrens während des allgemeinen Authentifizierungsprozesses denkbar.

Security-Token

Ähnlich dem TAN-Verfahren ist auch der Einsatz eines Security-Token zur eindeutigen Authentifizierung möglich. Bei diesem Verfahren erhält jeder Nutzer einen physischen Token, der speziell auf ihn autorisiert ist.

Token können nach zwei verschiedenen Prinzipien funktionieren; so kann ein Token ähnlich einem TAN-Generator auf einem eingebauten Bildschirm ein Einmal-Passwort anzeigen, welches vom Nutzer auf der Website einzugeben ist. Zum anderen kann ein Token in Form eines speziellen USB-Sticks eingerichtet werden, welcher geheime digitale Schlüssel enthält, die zur Authentifizierung nötig sind.

Bei beiden Möglichkeiten ist eine Authentifizierung nur dann möglich, wenn der Nutzer im Besitz des Tokens ist und zusätzlich sein Passwort kennt. Hierdurch wird ein sehr hoher Sicherheitsstandard gewährleistet, da Angreifer, die nicht im Besitz des Tokens sind, nur sehr geringe Chancen haben, in das entsprechende System einzudringen.

---

[194] Vgl. IT-Wissen (o.J.)

Als Nachteil kann an diesem Verfahren gesehen werden, dass es mit sehr hohen Kosten verbunden ist. Jeder Nutzer muss einen eigenen Token erhalten und zudem muss ein ständiger Support gewährleistet sein, für den Fall, dass ein Nutzer Probleme mit dem Einsatz seines Tokens hat.

5.3 Empfehlungen für das Unternehmen

Aufgrund der vorangegangenen Informationen und Analysen der AusweisApp und der BürgerApp kann dem Unternehmen im Folgenden eine Empfehlung ausgesprochen werden.

Im Falle der AusweisApp überwiegen die Schwächen und Gefahren in der Gegenüberstellung mit den Stärken und Möglichkeiten deutlich. Die Lösung ist nicht auf jedem Betriebssystem und Browser lauffähig, was die Nutzer möglicherweise stark einschränkt. Zudem ist der Sicherheitsaspekt ein großer Schwachpunkt der AusweisApp, da der verwendete Computer, das ausgewählte Kartenlesegerät und die AusweisApp selbst Gefahrenquellen für unbefugte Nutzung darstellen. Da der Quellcode der AusweisApp nicht öffentlich ist, können Fehlerquellen von unabhängiger Seite nicht ausgemacht werden, wodurch möglicherweise schwerwiegende Fehler im Programmcode Sicherheitslücken darstellen. Eine weitere Gefahrenquelle im Umgang mit der AusweisApp ist schließlich der Nutzer selbst, was eine Studie des HPI bestätigt. Viele Nutzer sind sich über die Verwendung der AusweisApp mit ihren Funktionen und Gefahren nicht im Klaren, womit auch hier Sicherheitsrisiken verursacht werden. Die Anwender werden bei der Anschaffung der AusweisApp nicht hinlänglich auf dessen Anwendung informiert, wodurch die Benutzerfreundlichkeit beeinträchtigt wird. Das weitaus größte Sicherheitsrisiko geht aus Sicht des Projektteams mit der fehlenden Zertifizierung der AusweisApp für das Unternehmen einher. Das BSI hat die AusweisApp bis heute nicht zertifiziert, womit die Rechtssicherheit nicht geklärt werden kann. Es wird zwar versichert, dass die AusweisApp bedenkenlos genutzt werden kann, jedoch muss die Verwendung der AusweisApp im Unternehmen ohne geklärte Rechtssicherheit als kritisch angesehen werden.

Die BürgerApp weist zunächst viele Stärken und Möglichkeiten auf. So zeichnet sie sich zum Beispiel durch eine einfache Implementierung, Komptabilität auf unterschiedlichen Betriebssystemen und eine intuitive Bedienung aus. Zudem ist der Quellcode des Programms öffentlich einzusehen, wodurch Fehlerquellen auch von unabhängiger Seite identifiziert werden können. Hiermit ist allerdings das Problem verbunden, dass dieser Programmcode kopiert und manipuliert werden kann und somit ein Missbrauch der BürgerApp gefördert wird. Der Support und die Administration der BürgerApp stellen eine Schwachstelle dar, die als bedeutend einzuschätzen ist. So gibt es derzeit kein Organisationsteam, das für Fragen, Anregun-

gen und Supportanfragen zur Verfügung steht. Außerdem liegen keine Erklärungen oder Anleitungen für den Nutzer bereit, was trotz einer intuitiven Bedienung der BürgerApp wünschenswert wäre. Des Weiteren befindet sich die BürgerApp im Entwicklungsstadium und ist somit, wie auch die AusweisApp, nicht zertifiziert, was die Rechtssicherheit der Anwendung beeinträchtigt.

Aus den genannten Gründen kommt das Projektteam zu dem Schluss, dass es dem Unternehmen zum heutigen Zeitpunkt keine Empfehlung für die Verwendung der AusweisApp oder der BürgerApp aussprechen kann. Vor allem der Aspekt der fehlenden Rechtssicherheit beider Alternativen lässt das Projektteam zu der Einschätzung kommen, dass eine Verwendung der AusweisApp oder der BürgerApp im Unternehmen zu Schwierigkeiten führen könnte.

Sobald die BSI die Softwarelösungen zertifiziert hat, tendiert das Projektteam zur Wahl der BürgerApp vom Open eCard Team, primär aus Gründen der Kompatibilität. Im Gegensatz zur AusweisApp ist die BürgerApp nahezu auf jedem gängigen Browser und Betriebssystem lauffähig, sodass im Umgang mit Kunden eine höhere Benutzerfreundlichkeit gewährleistet ist.

Zur Überbrückung bis zu einer erfolgreichen Zertifizierung einer der Anwendung sowie dem gestiegenem Zuspruch aus der Bevölkerung wird dem Unternehmen daher zum jetzigen Zeitpunkt empfohlen, sich wie in Kapitel 5.2 erläutert auf alternative Authentifizierungsverfahren zu stützen. Betrachtet wurden hier die Vergabe eines Passwortes in einem Online-Portal für jeden Kunden, der Einsatz eines TAN-Verfahrens und die Verwendung von Security Tokens. Security Tokens sind in der Anschaffung jedoch sehr kostspielig, weswegen diese Alternative nicht empfohlen wird. Eine bewährte Alternative ist das TAN-Verfahren, welches im Online-Banking Anwendung findet. Die Nutzung eines Online-Portals mittels Passwortanmeldung birgt einige Sicherheitsrisiken, was das Projektteam zu dem Schluss kommen lässt, dass die Einführung eines TAN-Verfahren dem Unternehmen zum aktuellen Zeitpunkt zu empfehlen ist.

6 Schlusswort

Die Einführung des neuen Personalausweises ermöglicht Bürgerinnen und Bürger mithilfe eines Kartenlesegeräts und einer Verbindungssoftware die Identifikation im Internet, um zunehmend angebotene Online-Dienste im Internet wahrzunehmen. Die Intention dieser neuen Authentifizierungsmethode ist die Verschärfung sicherheitstechnischer Aspekte, der Vereinfachung des elektronischen Einkaufs sowie eine Zeitersparnis, indem Behördengänge online getätigt werden können.

Nach einer Analyse der verfügbaren Schnittstellen zwischen dem Endanwender und dem Online-Authentifizierungsdienst wurde festgestellt, dass sowohl die vom Bundesministerium finanzierte Software „AusweisApp“ als auch die Open-Source entwickelte Alternative „Bürger-App“ vom Projekt „Open eCard“ zum momentanen Zeitpunkt noch erhebliche Defizite aufweisen. Auf Grundlage der vorgegangenen SWOT Analyse wird die Aussage getroffen, dass die Anwendungen vor allem in den Bereichen der Sicherheit und der Benutzerfreundlichkeit die gestellten Anforderungen noch nicht erfüllen. Insbesondere vor dem eingangs erwähnten Gesichtspunkt, dass die Online-Authentifizierung für den Schutz höchst sensibler Daten genutzt werden soll, wird ein enormes Maß an Datenschutz gefordert, das bisher von keiner der Applikationen erfüllt wird. Hinzu kommt die fehlende Rechtssicherheit bei Empfehlung der AusweisApp beziehungsweise BürgerApp, da es beiden an einer Zertifizierung durch das BSI mangelt.

Gleichzeitig mangelt es dem neuen Personalausweis allgemein an Akzeptanz in der Bevölkerung. Wie im ersten Teil der Arbeit dargelegt, findet die Online-Authentifizierung bei noch nicht einmal einem Drittel der Besitzer des neuen Dokuments Zuspruch, sodass sich auch hier eine Problematik für den Schutz des Online-Portals ergibt. Können nicht alle Kunden des Unternehmens den Zugang nutzen, bleibt ihnen der Zugang verwehrt oder es müssen alternative Anmelde-Verfahren angeboten werden. Aus diesem Grund empfiehlt sich zu diesem Zeitpunkt eher die Verwendung bewährter Sicherheitsmaßnahmen in Form von Passwörtern oder TAN-Verfahren.

Zusammenfassend lässt sich jedoch sagen, dass durch den neuen Personalausweise eine sichere, zuverlässige und einfache Authentifizierungsmethode geschaffen wird, sobald die Anwendungen die entsprechenden Anforderungen für die offizielle Zertifizierung erfüllen und der Personalausweis als Identifikationsmittel nicht nur anerkannt sondern auch entsprechend genutzt wird. Demnach sollte die Entwicklung der Einsatzbereiche und der Akzeptanz dieser Authentifizierungsmethode auch in Zukunft betrachtet werden, um rechtzeitig auf die entsprechende Methode umzusteigen.

Anhang

Anhangverzeichnis

Anhang 1: Prinzip der Online-Ausweisfunktion

Diensteanbieter
8 Authentisierung Nutzer
7 Datenübermittlung an Diensteanbieter
4 Anzeige abgefragter Daten
1 Aufruf der Website
2 Weiterleitung eID-Server
3 Chip- und Terminalauthentisierung
6 Datenübermittlung
5 Bestätigung PIN
Bürgerinnen und Bürger
eID-Server

Quellenverzeichnisse

Literaturverzeichnis

Adams, K. / Agesen, O. (2006): A Comparison of Software and Hardware Techniques for x86 Virtualization, in: Proceedings of the 12th international conference on Architectural support for programming languages and operating systems, Oktober 2006

Borges, G. u.a. (2011): Identitätsdiebstahl und Identitätsmissbrauch im Internet, Rechtliche und technische Aspekte, Heidelberg: Springer

Bundesministerium des Innern [Hrsg.] (2010): Alles Wissenswerte zum Personalausweis, 5. Auflage, Berlin: BMI

Horsch, M. u.a. (2013): Authentisierung mit der Open eCard App, Von Ausweiskarten zu datenschutzfreundlichen Credentials, in: DuD Datenschutz und Datensicherheit, Ausgabe 8/2013, S. 507-511

Hühnlein, D. u.a. (2012): On the design and implementation of the Open eCard App, in: Sicherheit, Suri, N. / Waidner, M. [Hrsg.], S. 95-110

Schröder, M. / Mogner, F. (2013): eID mit abgeleiteten Identitäten, in: DuD Datenschutz und Sicherheit, Ausgabe 8/2013, S. 530-534

Wiesmaier, A. (2013): Die Open eCard für mehr Transparenz, Vertrauen und Benutzerfreundlichkeit beim elektronischen Identitätsnachweis, Oktober 2012

Verzeichnis der Internet- und Intranet-Quellen

Anti-Botnet Beratungszentrum (2013): Sicherheitsrisiko Anwender: Nur 13% aller PCs "up-to-date", http://blog.botfrei.de/2013/04/sicherheitsrisiko-anwender-nur-13-aller-pcs-up-to-date/, Abruf: 21.12.2013

Asheuer, J./ u.a. (2013): Akzeptanz und Nutzerfreundlichkeit der AusweisApp; Eine qualitative Untersuchung, http://opus.kobv.de/ubp/volltexte/2013/6397/pdf/tbhpi69.pdf, Abruf: 31.12.2013

AusweisApp-Portal (o.J.a): AusweisApp für Ihr Betriebssystem, https://www.ausweisapp.bund.de/pweb/filedownload/download_pre.do, Abruf: 31.12.2013

AusweisApp-Portal (o.J.b): FAQ, Allgemein, https://www.ausweisapp.bund.de/pweb/cms/faq/02-Allgemein/index.jsp, Abruf: 31.12.2013

AusweisApp-Portal (o.J.c): FAQ Betriebssysteme, https://www.ausweisapp.bund.de/pweb/cms/faq/03-Betriebssysteme/index.jsp, Abruf: 13.12.2013

AusweisApp-Portal (o.J.d): Versionshistorie AusweisApp für Mac OS X, https://www.ausweisapp.bund.de/pweb/cms/filedownload/versionshistorie_MACOS.jsp, Abruf: 13.12.2013

AusweisApp-Portal (o.J.e): FAQ Browser, https://www.ausweisapp.bund.de/pweb/cms/faq/04-Browser/index.jsp, Abruf: 13.12.2013

AusweisApp-Portal (o.J.f): Von der AusweisApp unterstützte Lesegeräte, https://www.ausweisapp.bund.de/pweb/cms/kartenleser.jsp, Abruf: 13.12.2013

AusweisApp-Portal (o.J.g): FAQ Kartenleser, https://www.ausweisapp.bund.de/pweb/cms/faq/07-Kartenleser/index.jsp, Abruf: 13.12.2013

AusweisApp-Portal (o.J.h): FAQ Zertifizierung, https://www.ausweisapp.bund.de/pweb/cms/faq/02-Allgemein/08-Zertifizierung/index.jsp, Abruf: 21.12.2013

AusweisApp-Portal (o.J.i): FAQ, Online-Ausweisfunktion, https://www.ausweisapp.bund.de/pweb/cms/faq/09-Online-Ausweisfunktion/index.jsp, Abruf: 31.12.2013

AusweisApp-Portal (o.J.j): Support, Fragen, Fehlermeldungen, Probleme? – Hier gibt's Hilfe!, https://www.ausweisapp.bund.de/pweb/kontakt/kontakt_start_pre.do, Abruf: 31.12.2013

AusweisApp-Portal (o.J.k): Impressum, https://www.ausweisapp.bund.de/pweb/cms/impressum.jsp, Abruf: 31.12.2013

Baader, H. (2013): Open eCard stellt freie Alternative zur AusweisApp vor, http://www.pro-linux.de/news/1/19524/open-ecard-stellt-freie-alternative-zur-ausweisapp-vor.html, Abruf: 26.12.2013

Browser-Statistik (2013): Aktuelle Browser-Statistik, http://www.browser-statistik.de, Abruf: 14.12.2013

Bundesamt für Sicherheit in der Informationstechnik (o. J.a): Der neue Personalausweis, https://www.bsi-fuer-buer _ger.de/BSIFB/DE/SicherheitImNetz/Personalausweis/Personalausweis_node.html, Abruf: 08.12.2013

Bundesamt für Sicherheit in der Informationstechnik (o. J.b): Ausweisfunktion, https://www.bsi-fuer-buer _ger.de/BSIFB/DE/SicherheitImNetz/Personalausweis/Funktionen/Ausweisfunktion/ausweisfunktion_node.html, Abruf: 08.12.2013

Bundesamt für Sicherheit in der Informationstechnik (o.J.c): Wie mache ich meinen PC sicher?, https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/meinPC_node.html, Abruf: 14.12.2013

Bundesamt für Sicherheit in der Informationstechnik (o.J.d): Basisschutz für den Computer, https://www.bsi-fuer-buer-ger.de/BSIFB/DE/MeinPC/BasisschutzComputer/basisschutzComputer_node.html, Abruf: 14.12.2013

Bundesamt für Sicherheit in der Informationstechnik (o.J.e): Passwörter, https://www.bsi-fuerbuer-ger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html, Abruf: 14.12.2013

Bundesamt für Sicherheit in der Informationstechnik (o.J. f): BSI TR-03119 Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03119/index_htm.html, Abruf: 15.12.2013

Bundesamt für Sicherheit in der Informationstechnik (o. J. g): Fragen zum neuen Personalausweis, Fragen zur Technik und Sicherheit, https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Personalausweis/FAQ/FAQ_node.html#faq1529338, Abruf: 17.12.2013

Bundesamt für Sicherheit in der Informationstechnik (o. J. h): BSI TR-03112 Das eCard-API-Framework, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html, Abruf: 22.12.2013

Bundesministerium für Sicherheit in der Informationstechnik (o. J. i): BSI TR-03130 eID-Server, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html, Abruf: 21.01.2014

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (o.J.): Fernmeldegeheimnis, http://www.bfdi.bund.de/cln_029/nn_531474/DE/Themen/KommunikationsdiensteMedien/Telekommunikation/Artikel/Fernmeldegeheimnis.html__nnn=true, Abruf: 12.12.2013

Bundesdruckerei GmbH (2010): Der neue Personalausweis, Sicherheitsmerkmale, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Flyer-und-Broschueren/Flyer_Bundesdruckerei_Sicherheitsmerkmale_nPA.pdf?__blob=publicationFile, Abruf: 07.12.2013

Bundesdruckerei GmbH (2013a): Neuer Personalausweis, FAQs neuer Personalausweis, http://www.bundesdruckerei.de/de/1548-neuer-personalausweis, Abruf: 08.12.2013

Bundesdruckerei GmbH (2013b): Ausweis, Identitätsdokument für die reale und digitale Welt, http://www.bundesdruckerei.de/de/94-neuer-personalausweis, Abruf: 08.12.2013

Bundesdruckerei GmbH (2013c): Berechtigungszertifikate, http://www.bundesdruckerei.de/de/198-berechtigungszertifikate, Abruf: 08.12.2013

Bundesministerium der Justiz (o. J.): Gesetz über Personalausweise und den elektronischen Identitätsnachweis, Abschnitt 1, Allgemeine Vorschriften, § 5 Ausweismuster; gespeicherte Daten, http://www.gesetze-im-internet.de/pauswg/__5.html, Abruf : 07.12.2013

Bundesministerium des Innern (2013a): Anwendungen der Online- Ausweisfunktion – Wo kann ich die Funktion nutzen?, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Anwendungen_node.html, Abruf: 31.12.2013

Bundesministerium des Innern (2013b): Weitere Services, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Weitere-Services/Weitere-Services_node.html, Abruf: 31.12.2013

Bundesministerium des Innern (2013c): Der neue Ausweis, Anderes Format und neue Funktionen, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-neue-Ausweis/der-neue-Ausweis_node.html;jsessionid=EDF0A17656B521A2671F6F22460D399B.2_cid297, Abruf: 31.12.2013

Bundesministerium des Innern (2013d): Bürgerdienste – Anwendungen der Online-Ausweisfunktion, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Buergerdienste/Buergerdienste_node.html, Abruf: 07.12.2013

Bundesministerium des Innern (2013e): Der neue Ausweis, Neue Funktionen, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-neue-Ausweis/Funktionen/funktionen_node.html, Abruf: 07.12.2013

Bundesministerium des Innern (2013f): Online-Ausweisen mit dem neuen Personalausweis, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Online-Ausweisen_node.html, Abruf: 08.12.2013

Bundesministerium des Innern (2013g): Sicherheit und Datenschutz, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html, Abruf: 08.12.2013

Bundesministerium des Innern (2013h): Kartenlesegeräte, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Kartenlesegeraete/Kartenlesegeraete_node.html, Abruf: 12.12.2013

Bundesministerium des Innern (2013i): Zugang mit Pseudonym, http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/Einsatzmoeglichkeiten/Pseudonymer-Zugang/pseudonym_node.html, Abruf: 17.12.2013

Bundesministerium des Innern (2013j): Registrierung für ElsterOnline - einfach mit dem neuen Personalausweis, http://www.personalausweisportal.de/DE/Home/home_node.html, Abruf: 06.12.2013

Bundesministerium des Innern (2013k): Versicherungen – Anwendungen der Online-Ausweisfunktion, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Versicherungen/Versicherungen-node.html, Abruf: 06.12.2013

Bundesministerium des Innern (2013l): Finanzen – Anwendungen der Online-Ausweisfunktion, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Finanzen/Finanzen_node.html, Abruf: 12.12.2013

Bundesministerium des Innern (2013m): Weitere Services – Anwendungen der Online-Ausweisfunktion, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Weitere-Services/Weitere-Services_node.html, Abruf: 12.12.2013

Bundesministerium des Innern (2013n): Sicherheit und Datenschutz, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html, Abruf: 31.12.2013

Bundesministerium des Innern (2013o): Software, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Software/software-node.html, Abruf: 31.12.2013

Bundesministerium des Innern (2013p): Online- Ausweisen mit dem neuen Personalausweis, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Online-Ausweisen_node.html, Abruf: 31.12.2013

Bundesministerium des Innern (2013q): Online-Ausweisen – Das brauche ich: Software, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Software/software-node.html, Abruf: 26.12.2013

Bundesministerium des Innern (2012): Der neue Personalausweis – Informationen zur Online-Ausweisfunktion, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Flyer-und-Broschueren/eID_Broschuere.pdf?__blob=publicationFile, Abruf: 06.12.2013

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2010): Studie „Neuer Personalausweis“, Aktuelle Akzeptanz in der Bevölkerung, http://www.bitkom.org/files/documents/BITKOM_ePA_Extranet.pdf, Abruf: 12.12.2013

Bürger-App.de (2013): Die BürgerApp als AusweisApp zum selber programmieren, http://bürger-app.de/, Abruf: 26.12.2013

CHIP Digital GmbH (2013): Download Open eCard, http://www.chip.de/downloads/Open-eCard_62703934.html, Abruf: 24.12.2013

Computer Bild (2013): PSN: Sony setzt einige Passwörter zurück, http://www.computerbild.de/artikel/cbs-News-PS3-PSN-Sony-setzt-einige-Passwoerter-zurueck-9041871.html, Abruf: 08.01.2014

CSC (2012): Zwei Jahre neuer Personalausweis: Fünf Millionen Bundesbürger aktivieren elektronische Identität, Pressemitteilung vom 25.10.2012, http://www.csc.com/de/press_releases/90917-zwei_jahre_neuer_personalausweis_f%C3%BCnf_millionen_bundesb%C3%BCrger_aktivieren_elektronische_identit%C3%A4t, Abruf: 11.12.2013

Dietrich, C./Rossow, C./Pohlmann, N. (2010): Zwischenbericht: „Restrisiken beim Einsatz der AusweisApp auf dem Bürger-PC zur Online-Authentisierung mit Penetration- Test“, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/restrisiken.pdf?__blob=publicationFile, Abruf: 15.12.2013

Donath, A. (2013): Welche Programme nicht unter Mac OS X Mavericks laufen, http://www.golem.de/news/kompatibilitaetsliste-welche-programme-nicht-unter-mac-os-x-mavericks-laufen-1310-102404.html, Abruf: 13.12.2013

E-ID Client (2013): Was ist ein e-ID Client?, http://www.der-eid-client.de/?navigation=eid-client, Abruf: 21.01.2014

E-ID Funktion (o. J.): eID-Server bzw. eID-Service - Voraussetzung um die eID-Funktion des neuen Personalausweises (nPA) als Diensteanbieter bereitzustellen, http://www.die-eid-funktion.de/eid_server_bzw_eid_service_voraussetzung_um_die_eid_funktion_des_npa_bereitzustellen.php, Abruf: 21.01.2014

ELSTER (2013a): Willkommen bei ElsterOnline, Ihrem elektronischen Finanzamt!, https://www.elsteronline.de/eportal/Oeffentlich.tax, Abruf: 06.12.2013

ELSTER (2013b): Leistungen – ElsterOnline, https://www.elsteronline.de/eportal/Leistungen.tax, Abruf: 06.12.2013

Gartner (2007): Gartner Identifies the Top 10 Strategic Technologies for 2008, http://www.gartner.com/it/page.jsp?id=530109, Abruf: 02.07.2010

GDV Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2013): GDV-Maklerportal ist Meilenstein zur Förderung der elektronischen Kommunikation im Versicherungsvertrieb, http://www.gdv.de/2010/11/gdv-maklerportal-erfolgreich-gestartet-meilenstein-zur-foerderung-der-elektronischen-kommunikation-im-versicherungsvertrieb/, Abruf: 23.12.2013

Hengl, H. (2012): Die Online-Ausweisfunktion kämpft noch mit Anlaufschwierigkeiten, http://www.zdnet.de/88128131/die-online-ausweisfunktion-kampft-noch-mit-anlaufschwierigkeiten/, Abruf: 11.12.2013

Hühnlein, D. (2012): Open eCard App – Setup, kosmetik-1.0.0-pre2-SNAPSHOT-20121020.pptx, Folie 1, Abruf: 26.12.2013

Hühnlein, D. (2013a): Das Open eCard Projekt, Status und Ausblick, http://www.google.de/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&ved=0CDIQFjAA&url=http%3A%2F%2Fdev.openecard.org%2Fattachments%2Fdownload%2F231%2FDas-Open-eCard-Projekt-Status-und-Ausblick-2013-01-

30.ppt&ei=vcfPUqGkCY7ItAbbk4DgBw&usg=AFQjCNGRxUR7kjPHSYO5rcHqBq7zNqOtoQ&sig2=c3UrzUdZrqb-VYNM27i4Qg&bvm=bv.59026428,d.Yms, Abruf: 23.12.2013

Giga (2012): Apple-ID gehackt: Zahlreiche private Konten belastet, http://www.giga.de/unternehmen/apple/news/apple-id-gehackt-zahlreiche-private-konten-belastet/, Abruf: 08.01.2014

Hamburger Abendblatt (2009): 40 Prozent der WLANs nicht genug gesichert, http://www.abendblatt.de/ratgeber/wissen/article1217399/40-Prozent-der-WLANs-nicht-genug-gesichert.html, Abruf: 14.12.2013

Heise online (2013): Rechnungshof rügt BSI für AusweisApp-Schlamperei, http://www.heise.de/newsticker/meldung/Rechnungshof-ruegt-BSI-fuer-AusweisApp-Schlamperei-1848234.html, Abruf: 21.12.2013

Hühnlein, D. (2013b): Open eCard-Projekt veröffentlicht Basisversion für „BürgerApp“ und ruft zur Mitwirkung auf, Pressemitteilung, https://www.openecard.org/pr/2013-03-05.pdf, Abruf: 29.12.2013

Humpa, M. (o.J.): Download: Firefox, http://www.chip.de/downloads/Firefox_13014344.html, Abruf: 13.12.2013

IT-Wissen (o.J.): mTAN (mobile transaction number), http://www.itwissen.info/definition/lexikon/mobile-transaction-number-mTAN-Mobile-Transaktionsnummer.html, Abruf: 08.01.2013

Kämmer, Andreas (o. J.): Personalausweis Kartenlesegeräte, http://www.personalausweis-kartenlesegeraete.de/basis-kartenleser/, Abruf: 12.12.2013

Köhr, O. (2013): Chronologie des Überwachungsskandals, PRISM, „Tempora“ und viele Wanzen, http://www.tagesschau.de/ausland/chronologie-prism-tempora100.html, Abruf: 31.12.2013

Kubicek, Herbert (2011): Elektronischer Personalausweis, http://www.bpb.de/politik/innenpolitik/elektronischer-personalausweis/77634/elektronischer-personalausweis?p=0, Abruf: 11.12.2013

Kühne, A. (2013): Die Open eCard App für mehr Transparenz, Vertrauen und Benutzerfreundlichkeit, Präsentation auf der CeBIT im Rahmen des „Forums Open Source“, http://www.techcast.com/events/cebit13/sa-1000/?q=sa-1000, Abruf: 31.12.2013

Mozilla Developer Network (2013): HTTP access control (CORS), https://developer.mozilla.org/en-US/docs/HTTP/Access_control_CORS?redirectlocale=en-US&redirectslug=HTTP_access_control, Abruf: 30.12.2013

Open eCard Team (2013a): eCard-API-Framework, https://www.openecard.org/de/framework/eid-activation, Abruf: 27.12.2013

Open eCard Team (2013b): Download Android Open eCard App, https://www.openecard.org/de/download/android, Abruf: 26.12.2013

Open eCard Team (2013c): Open eCard, Download, https://www.openecard.org/de/download, Abruf: 29.12.2013

Pelz, W. (2004): SWOT-Analyse; Geschichte, Beispiele und Tipps zur Durchführung, http://wpelz.de/ress/swot.pdf, Abruf: 12.12.2013

Petrautzki, D. (2012): Open eCard Project – Android Download Requirements, README.txt, Abruf: 26.12.2013

Pommerening, K. (1991): Datenschutz und Datensicherheit, http://www.staff.uni-mainz.de/pommeren/Artikel/ds.pdf, Abruf: 12.12.2013

prolicon GROUP (2013): Pressemitteilung: procilon GROUP unterstützt Open e-Card Projekt, http://www.procilon.de/aktuelles/news/169-procilon-group-unterstuetzt-open-ecard-projekt, Abruf: 26.12.2013

Redmine (2013a): Project Open eCard Wiki – About the Open eCard App, https://dev.openecard.org/projects/open-ecard/wiki/User_Guide, Abruf: 26.12.2013

Redmine (2013b): Project Open eCard Documents – Rich Client, https://dev.openecard.org/documents/30, Abruf: 26.12.2013

Reiter, A. (2013): Neuer Personalausweis, Verwaltung als Motor, Kommune21, http://www.kommune21.de/meldung_15204_Verwaltung+als+Motor.html, Abruf: 11.12.2013

Seidel, U. (2011): Der neue Personalausweis, Physikalische Sicherheitsmerkmale, http://www.cio.bund.de/Web/DE/Strategische-Themen/IT-Investitionsprogramm/Aktivitaeten/CeBIT-2011/Vortraege/bka_dr_seidel_physikalische_sicherheits merkmale_des_npa_download.pdf?__blob=publicationFile, Abruf: 07.12.2013

Schejbal, J. (2011): Karten, Apps und Löcher – Ein Rückblick zum ePerso, http://janschejbal.wordpress.com/tag/ausweisapp/#epersoausweisapp, Abruf : 21.12.2013

Schumacher, F. (2012): OCA-Gestaltungsgrundsätze, http://dev.openecard.org/attachments/download/204/OCA-Gestaltungsgrunds%C3%A4tze.pdf, Abruf: 29.12.2013

Sietmann, Richard (2011): eID-Akzeptanz bleibt hinter den Erwartungen zurück, Heise Online, http://www.heise.de/newsticker/meldung/eID-Akzeptanz-bleibt-hinter-den-Erwartungen-zurueck-1171645.html, Abruf: 11.12.2013

Spiegel Online (2011): Neuer Personalausweis : Lesegerät-Hersteller warnt vor Simpel-Lesegerät, http://www.spiegel.de/netzwelt/gadgets/neuer-personalausweis-lesegeraet-hersteller-warnt-vor-simpel-lesegeraet-a-779437.html, Abruf: 21.12.2013

Stiftung Warentest (2011): Neuer Personalausweis: Enttäuschung im Praxistest, http://www.test.de/Neuer-Personalausweis-Enttaeuschung-im-Praxistest-4214969-0/, Abruf : 21.12.2013

TÜV Informationstechnik GmbH (o.J.): Technische Richtlinien des BSI, Konformitätsprüfung und Zertifizierung, https://www.tuvit.de/cps/rde/xbcr/SID-AD17E848-742ABFF9/tuevit_de/technische-richtlinien.pdf, Abruf: 15.12.2013

t3n (2012): Microsoft Store in Indien gehackt – Passwörter in Klartext gespeichert, http://t3n.de/news/microsoft-store-indien-gehackt-366118/, Abruf: 08.01.2013

ubuntuusers.de (2013): ElsterOnline, http://wiki.ubuntuusers.de/ElsterOnline, Abruf: 12.12.2013

Wieland, Thomas (2013): Feature #164, Implement grid layout concept, https://dev.openecard.org/boards/3/topics/45, Abruf: 29.12.2013

Windows (o.J.): InPrivate-Browsen, http://windows.microsoft.com/de-de/internet-explorer/products/ie-9/features/in-private, Abruf: 13.12.2013